

UNIVERSITÉ SIDI MOHAMED BEN ABDELLAH

SMA-SMI

FACULTÉ DES SCIENCES DHAR EL MEHRAZ

DÉPARTEMENT DE MATHÉMATIQUES

FES

POLYNÔMES



Pr MOMMED ZENNAYI

TABLE DES MATIÈRES

1-Séries formelles	1
1-1 Généralités.....	1
1-2 Valuation d'une série formelle.....	9
1-3 Dérivée d'une série formelle	13
1-4 Dérivées successives d'une série formelle.....	15
 2-Généralités sur les polynômes.....	18
2-1 Polynômes et degré d'un polynôme.....	18
2-2 Formule de Mac-Laurin.....	38
2-3 Formule de Taylor	39
 3-Division, divisibilité et fonctions polynômiales.	40
3-1 Division euclidienne.....	40
3-2 Développement suivant les puissances d'un polynôme.....	45
3-3 Procédé de Hörner.....	52
3-4 Divisibilité	54
3-5 Polynômes associés.....	59
3-6 Fonctions polynômiales.....	63
3-7 Division suivant les puissances croissantes.....	67

4-Arithmétique des polynômes.....	70
4-1 p.g.c.d de deux polynômes	70
4-2 Identité de Bezout et ses applications.....	80
4-3 Identité de Gauss et ses applications	82
4-4 p.p.c.m de deux polynômes	86
4-5 Polynômes irréductibles	92
4-6 Ordre de multiplicité.....	99
4-7 Factorisation.....	108

Polynômes

1-Séries formelles :

1-1- Généralités :

Définition 1-1-1 :

Soit A un anneau unitaire.

- Les suites d'éléments de A sont appelés les séries formelles à coefficients dans A .
- Si $f = (a_k)_{k \in \mathbb{N}} = (a_0, a_1, a_2, \dots) \in A^{\mathbb{N}}$ est une série formelle à coefficients dans A alors :
 - * les éléments a_k (tels que $k \in \mathbb{N}$) sont appelés les coefficients de f .
 - * Pour tout entier naturel k , a_k est appelé le coefficient de f de degré k .
 - * a_0 est appelé aussi le coefficient constant de f .
 - * Si $A = \mathbb{R}$ on dit aussi que f est à coefficients réels.
 - * Si $A = \mathbb{C}$ on dit aussi que f est à coefficients complexes.
- Dans l'ensemble $A^{\mathbb{N}}$ des séries formelles à coefficients dans A on définit les deux lois de composition internes suivantes :

$$\forall f = (a_k)_{k \in \mathbb{N}} \in A^{\mathbb{N}} \quad \text{et} \quad \forall g = (b_k)_{k \in \mathbb{N}} \in A^{\mathbb{N}} :$$

$$\left\{ \begin{array}{l} f + g = (a_k + b_k)_{k \in \mathbb{N}} \\ fg = (c_k)_{k \in \mathbb{N}} \quad \text{tq} : \forall k \in \mathbb{N} : c_k = \sum_{i=0}^k a_i b_{k-i} = \sum_{i+j=k} a_i b_j \end{array} \right.$$

Théorème 1-1-2 :

$(A^{\mathbb{N}}, +, \cdot)$ est un anneau unitaire dont l'unité est $(\delta_{0,k})_{k \in \mathbb{N}} = (1, 0, 0, \dots)$.

Démonstration :

- * Puisque $(A, +)$ est un groupe abélien alors $(A^{\mathbb{N}}, +)$ est un groupe abélien.
- * Soient $f = (a_k)_{k \in \mathbb{N}}$, $g = (b_k)_{k \in \mathbb{N}}$ et $h = (c_k)_{k \in \mathbb{N}}$ des séries formelles à coefficients dans A .
 Posons : $fg = (u_k)_{k \in \mathbb{N}}$, $gh = (v_k)_{k \in \mathbb{N}}$, $(fg)h = (d_k)_{k \in \mathbb{N}}$ et $f(gh) = (\delta_k)_{k \in \mathbb{N}}$.

$$\begin{aligned}
\forall k \in \mathbb{N} : d_k &= \sum_{i+j=k} u_i b_j = \sum_{i+j=k} \left(\sum_{p+q=i} a_p b_q \right) c_j = \sum_{i+j=k} \left(\sum_{p+q=i} a_p b_q c_j \right) \\
&= \sum_{p+q+j=k} a_p b_q c_j = \sum_{p+r=k} \sum_{q+j=r} a_p b_q c_j = \sum_{p+r=k} a_p \left(\sum_{q+j=r} b_q c_j \right) = \sum_{p+r=k} a_p v_r \\
&= \delta_k.
\end{aligned}$$

Par suite on a : $(fg)h = f(gh)$.

Donc la multiplication dans $A^{\mathbb{N}}$ est associative.

★ Soient $f = (a_k)_{k \in \mathbb{N}}$, $g = (b_k)_{k \in \mathbb{N}}$ et $h = (c_k)_{k \in \mathbb{N}}$ des séries formelles à coefficients dans A .

Posons : $f \cdot (g + h) = (d_k)_{k \in \mathbb{N}}$, $fg = (u_k)_{k \in \mathbb{N}}$, $fh = (v_k)_{k \in \mathbb{N}}$

$(g + h) \cdot f = (\delta_k)_{k \in \mathbb{N}}$, $gf = (r_k)_{k \in \mathbb{N}}$ et $fh = (s_k)_{k \in \mathbb{N}}$.

$$\bullet \forall k \in \mathbb{N} : d_k = \sum_{i=0}^k a_i (b_{k-i} + c_{k-i}) = \sum_{i=0}^k (a_i b_{k-i} + a_i c_{k-i}) = \sum_{i=0}^k a_i b_{k-i} + \sum_{i=0}^k a_i c_{k-i} = u_k + v_k.$$

Par suite on a : $f \cdot (g + h) = fg + fh$.

$$\bullet \forall k \in \mathbb{N} : \delta_k = \sum_{i=0}^k (b_i + c_i) a_{k-i} = \sum_{i=0}^k (b_i a_{k-i} + c_i a_{k-i}) = \sum_{i=0}^k b_i a_{k-i} + \sum_{i=0}^k c_i a_{k-i} = r_k + s_k.$$

Par suite on a : $(g + h)f = gf + hf$.

Donc la multiplication est distributive par rapport à l'addition dans $A^{\mathbb{N}}$.

★ Soit $f = (a_k)_{k \in \mathbb{N}}$ une série formelle à coefficients dans A .

Posons : $f \cdot (\delta_{0,k})_{k \in \mathbb{N}} = (u_k)_{k \in \mathbb{N}}$ et $(\delta_{0,k})_{k \in \mathbb{N}} \cdot f = (v_k)_{k \in \mathbb{N}}$.

$$\bullet \forall k \in \mathbb{N} : u_k = \sum_{i=0}^k a_i \delta_{0,k-i} = a_k \delta_{0,0} = a_k 1 = a_k. \text{ Alors : } f \cdot (\delta_{0,k})_{k \in \mathbb{N}} = f.$$

$$\bullet \forall k \in \mathbb{N} : v_k = \sum_{i=0}^k \delta_{0,i} a_{k-i} = \delta_{0,0} a_k = 1 a_k = a_k. \text{ Alors : } (\delta_{0,k})_{k \in \mathbb{N}} \cdot f = f.$$

Donc $(\delta_{0,k})_{k \in \mathbb{N}}$ est l'élément neutre de $A^{\mathbb{N}}$ pour la multiplication.

Ce qui montre que $(A^{\mathbb{N}}, +, \cdot)$ est un anneau unitaire dont l'unité est $(\delta_{0,k})_{k \in \mathbb{N}} = (1, 0, 0, \dots)$.

Théorème 1-1-3 :

L'application φ de A vers $A^{\mathbb{N}}$ définie par : $\varphi : A \rightarrow A^{\mathbb{N}}$

$$a \mapsto \varphi(a) = (a\delta_{0,k})_{k \in \mathbb{N}} = (a, 0, 0, \dots)$$

est un homomorphisme d'anneaux unitaire injectif.

Par conséquent :

* $\forall a \in A$: on confond $\varphi(a) = (a\delta_{0,k})_{k \in \mathbb{N}} = (a, 0, 0, \dots)$ avec a .

* On confond $\varphi(A)$ avec A et par suite A sera un sous anneau unitaire de $A^{\mathbb{N}}$.

Démonstration :

$$\begin{aligned}
\star \forall a, b \in A : \varphi(a + b) &= ((a + b)\delta_{0,k})_{k \in \mathbb{N}} = (a\delta_{0,k} + b\delta_{0,k})_{k \in \mathbb{N}} = (a\delta_{0,k})_{k \in \mathbb{N}} + (b\delta_{0,k})_{k \in \mathbb{N}} \\
&= \varphi(a) + \varphi(b).
\end{aligned}$$

★ $\forall a, b \in A$: posons $\varphi(a)\varphi(b) = (u_k)_{k \in \mathbb{N}}$.

$$\forall k \in \mathbb{N} : u_k = \sum_{i=0}^k (a\delta_{0,i})(b\delta_{0,k-i}) = \sum_{i=0}^k (ab)(\delta_{0,i}\delta_{0,k-i}).$$

- Si $k = 0$:

$$u_k = u_0 = \sum_{i=0}^0 (ab)(\delta_{0,i}\delta_{0,k-i}) = (ab)(\delta_{0,0}\delta_{0,0}) = (ab)(1 \cdot 1) = (ab)1 = (ab)\delta_{0,k}.$$

- Si $k \neq 0$:

$$u_k = (ab)(\delta_{0,0}\delta_{0,k}) = (ab)(1 \cdot 0) = (ab)0 = (ab)\delta_{0,k}.$$

Par suite on a : $\varphi(ab) = \varphi(a)\varphi(b)$.

★ $\varphi(1) = (1\delta_{0,k})_{k \in \mathbb{N}} = (\delta_{0,k})_{k \in \mathbb{N}}$.

★ Donc φ est un homomorphisme d'anneaux unitaire.

★ $\forall a \in \ker \varphi$: $\varphi(a) = (a\delta_{0,k})_{k \in \mathbb{N}}$ est nul.

$$\text{Alors : } [\forall k \in \mathbb{N} : a\delta_{0,k} = 0] \Rightarrow a = a1 = a\delta_{0,k} = 0$$

Par suite $\ker \varphi = \{0\}$.

Ce qui montre que φ est un homomorphisme d'anneaux unitaire injectif.

Par conséquent :

★ $\forall a \in A$: on confond $\varphi(a) = (a\delta_{0,k})_{k \in \mathbb{N}} = (a, 0, 0, \dots)$ avec a .

★ On confond $\varphi(A)$ avec A et par suite A sera un sous anneau unitaire de $A^{\mathbb{N}}$.

Notation 1-1-4 :

Soit A un anneau unitaire.

On note par X la série formelle à coefficients dans A définie par :

$$X = (\delta_{1,k})_{k \in \mathbb{N}} = (0, 1, 0, 0, \dots).$$

Propriétés et règles de calcul 1-1-5 :

Soit A un anneau unitaire.

1) $A^{\mathbb{N}}$ est nul si seulement si A est nul. C'est à dire : $A^{\mathbb{N}} = \{0\} \Leftrightarrow A = \{0\}$.

2) $A^{\mathbb{N}}$ est abélien si seulement si A est abélien.

3) Si A est non nul alors $X \neq 0$. C'est à dire : $A \neq \{0\} \Rightarrow X \in (A^{\mathbb{N}})^*$.

4) $\forall f = (a_k)_{k \in \mathbb{N}} \in A^{\mathbb{N}}$ et $\forall g = (b_k)_{k \in \mathbb{N}} \in A^{\mathbb{N}}$: si $fg = (c_k)_{k \in \mathbb{N}}$ alors :

$$\begin{cases} c_0 = a_0b_0 \\ c_1 = a_0b_1 + a_1b_0 \\ c_2 = a_0b_2 + a_1b_1 + a_2b_0 \\ \dots\dots\dots \end{cases}$$

$$5) \alpha \in A \text{ et } \forall f = (a_k)_{k \in \mathbb{N}} : \begin{cases} \alpha f = (\alpha a_k)_{k \in \mathbb{N}} \\ f \alpha = (a_k \alpha)_{k \in \mathbb{N}} \end{cases} :$$

$$6) \forall f = (a_k)_{k \in \mathbb{N}} \in A^{\mathbb{N}} : Xf = fX = (b_k)_{k \in \mathbb{N}} \text{ tq : } \begin{cases} b_0 = 0 \\ b_k = a_{k-1} \quad \forall k \in \mathbb{N}^* \end{cases}$$

C'est à dire : $Xf = fX = (0, a_0, a_1, a_2, \dots)$.

7) Si A est non nul alors X n'est pas inversible dans $A^{\mathbb{N}}$.

C'est à dire : $A \neq \{0\} \Rightarrow X \notin U(A^{\mathbb{N}})$.

8) $A^{\mathbb{N}}$ n'est pas un corps.

9) $\forall f = (a_k)_{k \in \mathbb{N}} \in A^{\mathbb{N}}$ et $\forall n \in \mathbb{N} : X^n f = f X^n = (b_k)_{k \in \mathbb{N}}$ tq :

$$\forall k \in \mathbb{N} : \begin{cases} b_k = 0 & \text{si } k < n \\ b_k = a_{k-n} & \text{si } k \geq n \end{cases}$$

10) $\forall n \in \mathbb{N} : X^n = (\delta_{n,k})_{k \in \mathbb{N}}$.

11) Si B est un sous-anneau unitaire de A alors $B^{\mathbb{N}}$ est un sous-anneau unitaire de $A^{\mathbb{N}}$.

En particulier $\mathbb{Z}^{\mathbb{N}}$ est un sous-anneau unitaire de $\mathbb{Q}^{\mathbb{N}}$, $\mathbb{Q}^{\mathbb{N}}$ est un sous-anneau unitaire de $\mathbb{R}^{\mathbb{N}}$ et $\mathbb{R}^{\mathbb{N}}$ est un sous-anneau unitaire de $\mathbb{C}^{\mathbb{N}}$.

12) Soient B un anneau unitaire, u un homomorphisme d'anneaux A vers B .

et $\tilde{u}$ l'application $A^{\mathbb{N}}$ vers $B^{\mathbb{N}}$ définie par :

$$\tilde{u} : A^{\mathbb{N}} \rightarrow B^{\mathbb{N}}$$

$$f = (a_k)_{k \in \mathbb{N}} \mapsto \tilde{u}(f) = (u(a_k))_{k \in \mathbb{N}}$$

a) $\tilde{u}$ est un homomorphisme d'anneaux de $A^{\mathbb{N}}$ vers $B^{\mathbb{N}}$ qui est unitaire si u est un homomorphisme d'anneaux unitaire.

b) $\tilde{u}$ est un prolongement de u à $A^{\mathbb{N}}$.

c) Si u est un homomorphisme d'anneaux unitaire alors $\tilde{u}(X) = X$.

d) $\ker(\tilde{u}) = \{f = (a_k)_{k \in \mathbb{N}} \in A^{\mathbb{N}} \text{ tq : } \forall k \in \mathbb{N} : a_k \in \ker(u)\} = \ker(u)^{\mathbb{N}}$.

e) $\tilde{u}$ est injectif si et seulement si u est injectif.

f) $\tilde{u}$ est surjectif si et seulement si u est surjectif.

g) $\tilde{u}$ est un isomorphisme de $A^{\mathbb{N}}$ vers $B^{\mathbb{N}}$ si et seulement si u est un isomorphisme de A vers B .

En particulier :

Si $A = B = \mathbb{C}$ et si u est l'automorphisme de $\mathbb{C}$ défini par : $\forall a \in \mathbb{C} : u(a) = \bar{a}$ alors :

i) $\forall f \in \mathbb{C}^{\mathbb{N}} : \tilde{u}(f)$ est noté : $\bar{f}$

ii) $\forall f, g \in \mathbb{C}^{\mathbb{N}} : [\overline{f+g} = \bar{f} + \bar{g} \text{ et } \overline{fg} = \bar{f}\bar{g}]$

iii) $\forall f \in \mathbb{C}^{\mathbb{N}} : f \in \mathbb{R}^{\mathbb{N}} \Leftrightarrow \bar{f} = f$

iv) $\tilde{u}$ est un automorphisme de $\mathbb{C}^{\mathbb{N}}$.

Démonstration :

1) $\Rightarrow$) **Si $A^{\mathbb{N}}$ est nul :**

Alors A est nul (car A est un sous anneau de $A^{\mathbb{N}} = \{0\}$).

$\Leftarrow$) **Si A est nul :**

Soit f une série formelle quelconque à coefficients dans A .

Puisque A est nul alors les coefficients de f sont tous nuls, par suite f est nul.

Donc $A^{\mathbb{N}}$ est nul.

2) $\Rightarrow$) **Si $A^{\mathbb{N}}$ est abélien :**

Alors A est abélien (car A est un sous anneau de $A^{\mathbb{N}}$).

$\Leftarrow$) **Si A est abélien :**

Soient $f = (a_k)_{k \in \mathbb{N}}$ et $g = (b_k)_{k \in \mathbb{N}}$ deux séries formelles à coefficients dans A .

Posons : $fg = (d_k)_{k \in \mathbb{N}}$ et $gf = (\delta_k)_{k \in \mathbb{N}}$.

$$\forall k \in \mathbb{N} : d_k = \sum_{i=0}^k a_i b_{k-i} = \sum_{i=0}^k b_{k-i} a_i = \sum_{j=0}^k b_j a_{k-j} = \delta_k.$$

Alors $fg = gf$.

Donc $A^{\mathbb{N}}$ est abélien.

3) Supposons que A est non nul.

$$\delta_{1,1} = 1 \neq 0 \text{ (car } A \text{ est non nul)} \Rightarrow X = (\delta_{1,k})_{k \in \mathbb{N}} \neq 0$$

4) Soient $f = (a_k)_{k \in \mathbb{N}}$ et $g = (b_k)_{k \in \mathbb{N}}$ deux séries formelles à coefficients dans A .

Posons $fg = (c_k)_{k \in \mathbb{N}}$.

$$\left\{ \begin{array}{l} c_0 = \sum_{i=0}^0 a_i b_{k-i} = a_0 b_0 \\ c_1 = \sum_{i=0}^1 a_i b_{k-i} = a_0 b_1 + a_1 b_0 \\ c_2 = \sum_{i=0}^2 a_i b_{k-i} = a_0 b_2 + a_1 b_1 + a_2 b_0 \\ \dots\dots\dots \end{array} \right.$$

5) Soient α un élément de K et $f = (a_k)_{k \in \mathbb{N}}$ une série formelle à coefficients dans A .

Posons $\alpha f = (c_k)_{k \in \mathbb{N}}$ et $f\alpha = (d_k)_{k \in \mathbb{N}}$. On a $\alpha = (\alpha\delta_{0,k})_{k \in \mathbb{N}}$

$$\forall k \in \mathbb{N} : \left\{ \begin{array}{l} c_k = \sum_{i=0}^k (\alpha\delta_{0,i}) a_{k-i} = (\alpha\delta_{0,0}) a_k = (\alpha 1) a_k = \alpha a_k \\ d_k = \sum_{i=0}^k a_i (\alpha\delta_{0,k-i}) = a_k (\alpha\delta_{0,0}) = a_k (\alpha 1) = a_k \alpha \end{array} \right. .$$

$$\text{Donc : } \left\{ \begin{array}{l} \alpha f = (\alpha a_k)_{k \in \mathbb{N}} \\ f \alpha = (a_k \alpha)_{k \in \mathbb{N}} \end{array} \right. :$$

6) Soit $f = (a_k)_{k \in \mathbb{N}}$ une série formelle à coefficients dans A .

Posons $Xf = (b_k)_{k \in \mathbb{N}}$ et $fX = (c_k)_{k \in \mathbb{N}}$.

$$\forall k \in \mathbb{N} : \left\{ \begin{array}{l} b_k = \sum_{i=0}^k (\delta_{1,i}) a_{k-i} \\ c_k = \sum_{i=0}^k a_i (\delta_{1,k-i}) \end{array} \right. .$$

- Pour $k = 0$:

$$\left\{ \begin{array}{l} b_0 = \sum_{i=0}^0 (\delta_{1,i}) a_{k-i} = \delta_{1,0} a_0 = 0 a_0 = 0 \\ c_0 = \sum_{i=0}^0 a_i (\delta_{1,k-i}) = a_0 \delta_{1,0} = a_0 0 = 0 \end{array} \right. \Rightarrow b_0 = c_0 = 0.$$

- **Pour $k \neq 0$:**

$$\begin{cases} b_k = \delta_{1,1} a_{k-1} = 1 a_{k-1} = a_{k-1} \\ c_k = a_{k-1} \delta_{1,1} = a_{k-1} 1 = a_{k-1} \end{cases} \Rightarrow b_k = c_k = a_{k-1}.$$

$$\text{Donc } Xf = fX = (b_k)_{k \in \mathbb{N}} \quad tq : \begin{cases} b_0 = 0 \\ b_k = a_{k-1} \quad \forall k \in \mathbb{N}^* \end{cases}.$$

C'est à dire : $Xf = fX = (0, a_0, a_1, a_2, \dots)$.

7) Supposons que A est non nul et que X est inversible dans $A^{\mathbb{N}}$.

Posons $X^{-1} = (u_k)_{k \in \mathbb{N}}$

Puisque $XX^{-1} = 1 = (\delta_{0,k})_{k \in \mathbb{N}}$ alors : $1 = \delta_{0,0} = 0$ (d'après 6)). Ce qui est absurde.

Donc X n'est pas inversible dans $A^{\mathbb{N}}$.

C'est à dire : $A \neq \{0\} \Rightarrow X \notin U(A^{\mathbb{N}})$.

8) - **Si A est nul :**

Alors $A^{\mathbb{N}}$ n'est pas nul. Donc $A^{\mathbb{N}}$ n'est pas un corps.

- **Si A n'est pas nul :**

Puisque (d'après 3)) X n'est pas nul et puisque (d'après 7)) X n'est pas inversible dans $A^{\mathbb{N}}$ alors $A^{\mathbb{N}}$ n'est pas un corps.

9) Soit $f = (a_k)_{k \in \mathbb{N}}$ une série formelle à coefficients dans A .

Montrons par récurrence que pour tout entier naturel n , $X^n f = f X^n = (b_k)_{k \in \mathbb{N}}$

tel que :

$$\forall k \in \mathbb{N} : \begin{cases} b_k = 0 & \text{si } k < n \\ b_k = a_{k-n} & \text{si } k \geq n \end{cases}.$$

- **Pour $n = 0$:**

$$X^0 f = X^0 f = 1f = f1 = fX^0 = fX^n.$$

Posons $X^n f = f X^n = (b_k)_{k \in \mathbb{N}}$. Alors : $(b_k)_{k \in \mathbb{N}} = X^n f = X^0 f = 1f = f = (a_k)_{k \in \mathbb{N}}$.

$$\text{On a donc : } \forall k \in \mathbb{N} : b_k = a_k \Rightarrow \begin{cases} b_k = 0 & \text{si } k < 0 = n \\ b_k = a_{k-0} = a_{k-n} & \text{si } k \geq 0 = n \end{cases}.$$

- **Pour $n = 1$:**

Supposons que $X^{n-1} f = f X^{n-1}$ et que si $X^{n-1} f = f X^{n-1} = (b_k)_{k \in \mathbb{N}}$ alors :

$$\forall k \in \mathbb{N} : \begin{cases} b_k = 0 & \text{si } k < n-1 \\ b_k = a_{k-n} & \text{si } k \geq n-1 \end{cases}.$$

- **Pour n :**

Montrons qu'alors $X^n f = f X^n$ et que si $X^n f = f X^n = (b_k)_{k \in \mathbb{N}}$ alors :

$$\forall k \in \mathbb{N} : \begin{cases} b_k = 0 & \text{si } k < n \\ b_k = a_{k-n} & \text{si } k \geq n \end{cases}.$$

Posons : $X^n f = (b_k)_{k \in \mathbb{N}}$ et $X^{n-1} f = (d_k)_{k \in \mathbb{N}}$.

D'après l'hypothèse de récurrence $X^{n-1} f = f X^{n-1}$ et on a :

$$\forall k \in \mathbb{N} : \begin{cases} d_k = 0 & \text{si } k < n-1 \\ d_k = a_{k-n} & \text{si } k \geq n-1 \end{cases}.$$

$$\begin{aligned} \star X^n f &= f X^n = (XX^{n-1}) f = X(X^{n-1} f) = X(f X^{n-1}) = (Xf) X^{n-1} \\ &= (fX) X^{n-1} = f(XX^{n-1}) = f X^n. \end{aligned}$$

★ Puisque $X^{n-1}f = (d_k)_{k \in \mathbb{N}}$ et puisque $X(X^{n-1}f) = X^n f = (b_k)_{k \in \mathbb{N}}$ alors,

$$\text{d'après 6) on a : } \begin{cases} b_0 = 0 \\ b_k = d_{k-1} \quad \forall k \in \mathbb{N}^* \end{cases}.$$

Soit k un entier naturel quelconque.

• **Si $k = 0$:**

Alors : $k = 0 < n$ et $b_k = b_0 = 0$.

• **Si $1 \leq k < n$:**

Alors : $0 \leq k-1 < n-1$ et $b_k = d_{k-1} = 0$.

• **Si $k \geq n$:**

Alors : $k-1 \geq n-1$ et $b_k = d_{k-1} = a_{k-1-(n-1)} = a_{k-1-n+1} = a_{k-n}$.

Ce qui montre que :

$$\forall k \in \mathbb{N} : \begin{cases} b_k = 0 & \text{si } k < n \\ b_k = a_{k-n} & \text{si } k \geq n \end{cases}$$

10) Soit n un entier naturel quelconque.

Posons $X^n = (b_k)_{k \in \mathbb{N}}$, alors : $(b_k)_{k \in \mathbb{N}} = X^n = X^n 1 = X^n \cdot (\delta_{0,k})_{k \in \mathbb{N}}$.

Soit k un entier naturel quelconque.

- **Si $k < n$:**

Alors (d'après 9)), $b_k = 0 = \delta_{n,k}$ (car $k \neq n$).

- **Si $k > n$:**

Alors (d'après 9)), $b_k = \delta_{0,k-n} = 0 = \delta_{n,k}$.

- **Si $k = n$:**

Alors (d'après 9)), $b_k = \delta_{0,k-n} = \delta_{0,n-n} = \delta_{0,0} = 1 = \delta_{n,n} = \delta_{n,k}$.

Donc : $X^n = (\delta_{n,k})_{k \in \mathbb{N}}$.

11) $B^{\mathbb{N}}$ est un sous-anneau unitaire de $A^{\mathbb{N}}$ (car $B^{\mathbb{N}} \subset A^{\mathbb{N}}$).

En particulier $\mathbb{Z}^{\mathbb{N}}$ est un sous-anneau unitaire de $\mathbb{Q}^{\mathbb{N}}$, $\mathbb{Q}^{\mathbb{N}}$ est un sous-anneau unitaire de $\mathbb{R}^{\mathbb{N}}$ et $\mathbb{R}^{\mathbb{N}}$ est un sous-anneau unitaire de $\mathbb{C}^{\mathbb{N}}$.

12) a) ★ Soient $f = (a_k)_{k \in \mathbb{N}}$ et $g = (b_k)_{k \in \mathbb{N}}$ deux séries formelles à coefficients dans A .

$$\begin{aligned} \bullet \tilde{u}(f+g) &= (u(a_k + b_k))_{k \in \mathbb{N}} = (u(a_k) + u(b_k))_{k \in \mathbb{N}} = (u(a_k))_{k \in \mathbb{N}} + (u(b_k))_{k \in \mathbb{N}} \\ &= \tilde{u}(f) + \tilde{u}(g). \end{aligned}$$

$$\bullet \text{ Posons : } fg = (c_k)_{k \in \mathbb{N}} \text{ et } \tilde{u}(f)\tilde{u}(g) = (d_k)_{k \in \mathbb{N}}.$$

$$fg = (c_k)_{k \in \mathbb{N}} \Rightarrow \tilde{u}(fg) = (u(c_k))_{k \in \mathbb{N}}.$$

$$\forall k \in \mathbb{N} : u(c_k) = u\left(\sum_{i=0}^k a_i b_{k-i}\right) = \sum_{i=0}^k u(a_i)u(b_{k-i}) = d_k.$$

$$\text{On a alors : } \tilde{u}(fg) = \tilde{u}(f)\tilde{u}(g).$$

Donc $\tilde{u}$ est un homomorphisme d'anneaux de $A^{\mathbb{N}}$ vers $B^{\mathbb{N}}$.

★ Supposons que u est un homomorphisme d'anneaux unitaire.

$$\tilde{u}(1_A) = \tilde{u}((\delta_{0,k})_{k \in \mathbb{N}}) = (u(\delta_{0,k}))_{k \in \mathbb{N}} = (\delta_{0,k})_{k \in \mathbb{N}} = 1_B.$$

Ce qui montre que $\tilde{u}$ est un homomorphisme d'anneaux unitaire de $A^{\mathbb{N}}$ vers $B^{\mathbb{N}}$.

$$\text{b) } \forall a \in K : \begin{cases} u(a\delta_{0,k}) = u(a0_A) = u(0_A) = 0_B = u(a)0_B = u(a)\delta_{0,k} \quad \forall k \in \mathbb{N}^* \\ u(a\delta_{0,0}) = u(a1_A) = u(a) = u(a)1_B = u(a)\delta_{0,0} \end{cases}.$$

$$\text{Par suite on a : } \forall k \in \mathbb{N} : u(a\delta_{0,k}) = u(a)\delta_{0,k}.$$

Alors : $\tilde{u}(a) = \tilde{u}((a\delta_{0,k})_{k \in \mathbb{N}}) = (u(a\delta_{0,k}))_{k \in \mathbb{N}} = (u(a)\delta_{0,k})_{k \in \mathbb{N}} = u(a)$.

Donc $\tilde{u}$ est un prolongement de u à $A^{\mathbb{N}}$.

c) Supposons que u est un homomorphisme d'anneaux unitaire.

$$\tilde{u}(X) = \tilde{u}((\delta_{1,k})_{k \in \mathbb{N}}) = (u(\delta_{1,k}))_{k \in \mathbb{N}} = (\delta_{1,k})_{k \in \mathbb{N}} = X.$$

d) Soit $f = (a_k)_{k \in \mathbb{N}}$ une série formelle à coefficients dans A .

$$f = (a_k)_{k \in \mathbb{N}} \in \ker(\tilde{u}) \Leftrightarrow \tilde{u}(f) = 0_B \Leftrightarrow (u(a_k))_{k \in \mathbb{N}} = 0_B$$

$$\Leftrightarrow \forall k \in \mathbb{N} : u(a_k) = 0_B$$

$$\Leftrightarrow \forall k \in \mathbb{N} : a_k \in \ker(u).$$

$$\text{Donc } \ker(\tilde{u}) = \{f = (a_k)_{k \in \mathbb{N}} \in A^{\mathbb{N}} \text{ tq : } \forall k \in \mathbb{N} : a_k \in \ker(u)\} = \ker(u)^{\mathbb{N}}.$$

e) $\Rightarrow$) **Si $\tilde{u}$ est injectif :**

$$\forall a \in \ker(u) : \tilde{u}(a) = u(a) = 0 \Rightarrow a \in \ker(\tilde{u}) = \{0\} \Rightarrow a = 0.$$

Alors : $\ker(u) = \{0\}$. Donc u est injectif.

$\Leftarrow$) **Si u est injectif :**

$$\begin{aligned} \text{Alors : } \ker(\tilde{u}) &= \{f = (a_k)_{k \in \mathbb{N}} \in A^{\mathbb{N}} \text{ tq : } \forall k \in \mathbb{N} : a_k \in \ker(u) = \{0\}\} \\ &= \{f = (a_k)_{k \in \mathbb{N}} \in A^{\mathbb{N}} \text{ tq : } \forall k \in \mathbb{N} : a_k = 0\} \\ &= \{0\}. \end{aligned}$$

Donc $\tilde{u}$ est injectif.

f) $\Rightarrow$) **Si $\tilde{u}$ est surjectif :**

$$\forall b \in B : \exists f = (a_k)_{k \in \mathbb{N}} \in A^{\mathbb{N}} \text{ tq : } b = \tilde{u}(f).$$

$$\text{Alors : } (b\delta_{0,k})_{k \in \mathbb{N}} = (u(a_k))_{k \in \mathbb{N}} \Rightarrow b = b1 = b\delta_{0,0} = u(a_0).$$

Ce qui montre que u est surjectif.

$\Leftarrow$) **Si u est surjectif :**

Soit $g = (b_k)_{k \in \mathbb{N}}$ une série formelle à coefficients dans A .

$$\forall k \in \mathbb{N} : \exists a_k \in A \text{ tq : } b_k = u(a_k) \text{ (car } u \text{ est surjectif).}$$

$$\text{Posons } f = (a_k)_{k \in \mathbb{N}} \in A^{\mathbb{N}}.$$

$$\text{On a alors : } g = (b_k)_{k \in \mathbb{N}} = (u(a_k))_{k \in \mathbb{N}} = \tilde{u}(f).$$

Ce qui montre que $\tilde{u}$ est surjectif.

g) [$\tilde{u}$ est un isomorphisme de $A^{\mathbb{N}}$ vers $B^{\mathbb{N}}$]

$$\Leftrightarrow [\tilde{u} \text{ est injectif et surjectif}]$$

$$\Leftrightarrow [u \text{ est injectif et surjectif}] \text{ (d'après e) et f)}$$

$$\Leftrightarrow [u \text{ est un isomorphisme de } A \text{ vers } B].$$

En particulier :

Si $A = B = \mathbb{C}$ et si u est l'automorphisme de $\mathbb{C}$ défini par : $\forall a \in \mathbb{C} : u(a) = \bar{a}$ alors :

i) $\forall f \in \mathbb{C}^{\mathbb{N}} : \tilde{u}(f)$ est noté $\bar{f}$

$$\text{ii) } \forall f, g \in \mathbb{C}^{\mathbb{N}} : \begin{cases} \overline{f+g} = \tilde{u}(f+g) = \tilde{u}(f) + \tilde{u}(g) = \bar{f} + \bar{g} \\ \overline{fg} = \tilde{u}(fg) = \tilde{u}(f)\tilde{u}(g) = \bar{f}\bar{g} \end{cases}.$$

iii) Soit $f = (a_k)_{k \in \mathbb{N}}$ une série formelle à coefficients complexe.

$$f \in \mathbb{R}^{\mathbb{N}} \Leftrightarrow [\forall k \in \mathbb{N} : a_k \in \mathbb{R}] \Leftrightarrow [\forall k \in \mathbb{N} : \bar{a}_k = a_k] \Leftrightarrow [\forall k \in \mathbb{N} : u(a_k) = a_k]$$

$$\Leftrightarrow \tilde{u}(f) = f$$

$$\Leftrightarrow \bar{\bar{f}} = f$$

iv) Puisque u est un automorphisme de $\mathbb{C}$ alors $\tilde{u}$ est un automorphisme de $\mathbb{C}^{\mathbb{N}}$.

1-2- Valuation d'une série formelle :

Définition 1-2-1 :

Soit A un anneau unitaire et $f = (a_k)_{k \in \mathbb{N}} \in A^{\mathbb{N}}$ une série formelle à coefficients dans A .

- Si $f \neq 0$:

Le plus petit entier naturel k tel que $a_k \neq 0$ est appelé la valuation de f et noté $v(f)$.

C'est à dire : $v(f) = \min(\{k \in \mathbb{N} \mid a_k \neq 0\})$.

- Si $f = 0$:

On pose $v(0) = +\infty$ appelé la valuation de 0.

Propriétés 1-2-2 :

Soient A un anneau unitaire et $f = (a_k)_{k \in \mathbb{N}}$ une série formelle à coefficients dans A .

1) $v(f) \in \mathbb{N} \Leftrightarrow f \neq 0$.

2) $v(f) = +\infty \Leftrightarrow f = 0$.

3) $v(f) \in \mathbb{N} \cup \{+\infty\}$.

4) $v(f) = 0 \Leftrightarrow a_0 \neq 0$.

5) $\forall n \in \mathbb{N} : v(f) = n \Leftrightarrow \begin{cases} a_n \neq 0 \\ \forall k \in \mathbb{N} : k < n \Rightarrow a_k = 0 \end{cases}$.

6) $\forall n \in \mathbb{N} : v(f) \geq n \Leftrightarrow [\forall k \in \mathbb{N} : k < n \Rightarrow a_k = 0]$.

En effet :

1) $\Rightarrow$) Si $v(f) \in \mathbb{N}$:

Supposons que $f = 0$.

D'après la définition 1-2-1, $v(f) = +\infty \notin \mathbb{N}$. Ce qui est absurde. Donc $f \neq 0$.

$\Leftarrow$) Si $f \neq 0$:

Soit n le plus petit entier naturel k tel que $a_k \neq 0$.

D'après la définition 1-2-1 : $v(f) = n \in \mathbb{N}$.

2) $\Rightarrow$) Si $v(f) = +\infty$:

$v(f) = +\infty \notin \mathbb{N} \Rightarrow f = 0$ (d'après 1)).

$\Leftarrow$) Si $f = 0$:

D'après la définition 1-2-1 : $v(f) = +\infty$.

3) - Si $f \neq 0$: $v(f) \in \mathbb{N} \subset \mathbb{N} \cup \{+\infty\}$.

- Si $f = 0$: $v(f) = +\infty \in \mathbb{N} \cup \{+\infty\}$.

Donc : $v(f) \in \mathbb{N} \cup \{+\infty\}$.

4) $\Rightarrow$) Si $v(f) = 0$:

Alors 0 est le plus petit entier naturel k tel que $a_k \neq 0$. Donc $a_0 \neq 0$.

$\Leftarrow$) Si $a_0 \neq 0$:

$a_0 \neq 0 \Rightarrow f \neq 0 \Rightarrow v(f) \in \mathbb{N} \Rightarrow v(f) \geq 0$.

$a_0 \neq 0 \Rightarrow v(f) \leq 0$.

Donc : $v(f) = 0$.

5) Soient n un entier naturel et $I = \{k \in \mathbb{N} \mid a_k \neq 0\}$

$\Rightarrow$) Si $v(f) = n$:

Puisque $v(f) = n \in \mathbb{N}$ alors f est non nulle et $n = v(f)$ est le petit élément de I .

Donc : $\begin{cases} n \in I \\ \forall k \in \mathbb{N} : k < n \Rightarrow k \notin I \end{cases} \Rightarrow \begin{cases} a_n \neq 0 \\ \forall k \in \mathbb{N} : k < n \Rightarrow a_k = 0 \end{cases}$.

$\Leftarrow$) Si $a_n \neq 0$ et si on a pour tout entier naturel $k < n$, $a_k = 0$:

Posons $v(f) = m$.

Puisque $a_n \neq 0$ alors f est non nulle, $m = v(f) \in \mathbb{N}$, m est le plus petit élément de I , et $n \in I$.

$n \in I \Rightarrow m \leq n$.

Supposons que $m < n$. Alors : $a_m = 0 \Rightarrow v(f) = m \notin I$. Ce qui est absurde.

Donc $v(f) = m = n$.

6) Soient n un entier naturel et posons $v(f) = m$.

$\Rightarrow$) Si $v(f) \geq n$:

- Si $v(f) = +\infty$:

Alors f est nulle. On donc : $\forall k \in \mathbb{N} : k < n \Rightarrow a_k = 0$.

- Si $v(f) \neq +\infty$:

Alors f est non nulle. $\forall k \in \mathbb{N}$ tq : $k < n$.

$k < n \Rightarrow k < m \Rightarrow a_k = 0$.

$\Leftarrow$) Si on a pour tout entier naturel $k < n$, $a_k = 0$:

Posons $v(f) = m$ et supposons $m < n$.

Alors $m \in \mathbb{N}$ et $a_m = 0$. Donc $m \neq v(f)$. Ce qui est absurde.

Ce qui montre que $v(f) = m \geq n$.

Exemple 1-2-3 :

Soit A un anneau unitaire non nul.

1) $\forall a \in A^* : v(a) = 0$.

2) $v(X) = 1$.

3) $\forall n \in \mathbb{N} : v(X^n) = n$.

En effet :

1) Soit a un élément non nul de K .

Puisque $a = (a\delta_{0,k})_{k \in \mathbb{N}}$ et puisque $a\delta_{0,0} = a1 = a \neq 0$ alors (d'après la propriétés 1-2-2 4)) $v(a) = 0$.

2) Puisque $X = (\delta_{1,k})_{k \in \mathbb{N}}$, $\delta_{1,1} = 1 \neq 0$ et $\delta_{0,0} = 0$ alors (d'après la propriétés 1-2-2 5)) $v(X) = 1$.

3) Soit n un entier naturel.

Puisqu'on a :
$$\begin{cases} X^n = (\delta_{n,k})_{k \in \mathbb{N}} \\ \delta_{n,n} = 1 \neq 0 \\ \forall k \in \mathbb{N} : k < n \Rightarrow \delta_{n,k} = 0 \end{cases} \quad \text{alors } v(X^n) = n.$$

Propriétés 1-2-4 :

Soient A un anneau unitaire.

1) $\forall f, g \in A^{\mathbb{N}}$:

a) $v(f+g) \geq \min(v(f), v(g))$.

b) $v(f) \neq v(g) \Rightarrow v(f+g) = \min(v(f), v(g))$.

2) $\forall f \in A^{\mathbb{N}}$ et $\forall n \in \mathbb{N} : v(f) = n \Leftrightarrow \exists f_0 \in A^{\mathbb{N}}$ tq :
$$\begin{cases} f = X^n f_0 \\ v(f_0) = 0 \end{cases}.$$

3) $\forall f \in A^{\mathbb{N}}$ et $\forall n \in \mathbb{N} : v(f) \geq n \Leftrightarrow \exists f_0 \in A^{\mathbb{N}}$ tq : $f = X^n f_0$.

$$4) \forall f, g \in A^{\mathbb{N}} : v(fg) \geq v(f) + v(g).$$

5) Si A est intègre et si f, g sont des séries formelles à coefficients dans A alors :

a) $v(f) = v(g) = 0 \Rightarrow v(fg) = 0.$

b) $v(fg) = v(f) + v(g).$

Démonstration :

1) Soient $f = (a_k)_{k \in \mathbb{N}}$ et $g = (b_k)_{k \in \mathbb{N}}$ deux séries formelles à coefficients dans A .

a) Posons $\min(v(f), v(g)) = n$.

- Si $f = 0$:

$$\begin{aligned} \text{Alors : } v(f+g) &= v(0+g) = v(g) = \min(+\infty, v(g)) = \min(v(0), v(g)) \\ &= \min(v(f), v(g)) \geq \min(v(f), v(g)). \end{aligned}$$

- Si $g = 0$:

$$\begin{aligned} \text{Alors : } v(f+g) &= v(f+0) = v(f) = \min(v(f), +\infty) = \min(v(0), v(g)) \\ &= \min(v(f), v(g)) \geq \min(v(f), v(g)). \end{aligned}$$

- Si $f \neq 0$ et $g \neq 0$:

$\forall k \in \mathbb{N}$ tq : $k < n$ on a :

$$\begin{cases} k < n = \min(v(f), v(g)) \leq v(f) \Rightarrow a_k = 0 \\ k < n = \min(v(f), v(g)) \leq v(g) \Rightarrow b_k = 0 \end{cases} \Rightarrow a_k + b_k = 0.$$

Donc : $v(f+g) \geq n = \min(v(f), v(g)).$

b) Supposons que $v(f) \neq v(g)$ et posons $\min(v(f), v(g)) = n$.

$$v(f) \neq v(g) \Rightarrow n = \min(v(f), v(g)) \neq +\infty \Rightarrow n \in \mathbb{N}.$$

$$v(f) \neq v(g) \Rightarrow [v(f) < v(g) \text{ ou } v(g) < v(f)].$$

D'après a) on a : $v(f+g) \geq n = \min(v(f), v(g)).$

- Si $v(f) < v(g)$:

$$\begin{aligned} \text{Alors : } \begin{cases} v(f) = n \\ n < v(g) \end{cases} &\Rightarrow \begin{cases} a_n \neq 0 \\ b_n = 0 \end{cases} \Rightarrow a_n + b_n = a_n \neq 0 \\ &\Rightarrow v(f+g) \leq n = \min(v(f), v(g)). \end{aligned}$$

- Si $v(g) < v(f)$:

$$\begin{aligned} \text{Alors : } \begin{cases} n < v(f) \\ v(g) = n \end{cases} &\Rightarrow \begin{cases} a_n = 0 \\ b_n \neq 0 \end{cases} \Rightarrow a_n + b_n = b_n \neq 0 \\ &\Rightarrow v(f+g) \leq n = \min(v(f), v(g)). \end{aligned}$$

Puisque $v(f+g) \geq n = \min(v(f), v(g))$ et $v(f+g) \leq n = \min(v(f), v(g))$ alors :

$$v(f+g) = n = \min(v(f), v(g)).$$

2) Soient $f = (a_k)_{k \in \mathbb{N}}$ une série formelle à coefficients dans A et n un entier naturel.

$\Rightarrow$) Si $v(f) = n$:

Alors : $a_n \neq 0$ et $\forall k < n : a_k = 0.$

Pour tout entier naturel k , posons $d_k = a_{n+k}$ et posons $f_0 = (d_k)_{k \in \mathbb{N}}$.

$$d_0 = a_{n+0} = a_n \neq 0 \Rightarrow v(f_0) = 0.$$

Posons $X^n f_0 = (b_k)_{k \in \mathbb{N}}$.

Pour tout entier naturel k on a :

- Si $k < n$: $b_k = 0 = a_k.$

- Si $k \geq n$: $b_k = d_{k-n} = a_{n+k-n} = a_k.$

$$\text{Par suite on a : } \begin{cases} f = X^n f_0 \\ v(f_0) = 0 \end{cases}.$$

⇐) Supposons qu'il existe une série formelle f_0 à coefficients dans A telle que $f = X^n f_0$ et $v(f_0) = 0$.

Posons $f_0 = (d_k)_{k \in \mathbb{N}}$. $v(f_0) = 0 \Rightarrow d_0 \neq 0$.

Par suite on a :
$$\begin{cases} a_n = d_{n-n} = d_0 \neq 0 \\ \forall k \in \mathbb{N} : k < n \Rightarrow a_k = 0 \end{cases}.$$

Donc $v(f) = n$.

3) Soient f une série formelle à coefficients dans A et n un entier naturel.

Supposons que $v(f) \geq n$.

Posons $v(f) = m$.

- Si $m = +\infty$:

Alors $v(f) = m = +\infty \Rightarrow f = 0$.

Il suffit de prendre $f_0 = 0$ et on a : $f = 0 = X^n 0 = X^n f_0$.

- Si $m \neq +\infty$:

Alors $v(f) = m \in \mathbb{N}$.

D'après 2) il existe une série formelle f_0 à coefficients dans A telle que

$f = X^m g$ et $v(g) = 0$.

$m = v(f) \geq n \Rightarrow m - n \in \mathbb{N}$.

$f = X^m g = X^{n+m-n} g = (X^n X^{m-n}) g = X^n (X^{m-n} g)$.

Il suffit de prendre $f_0 = X^{m-n} g$ et on a :
$$\begin{cases} f_0 \in A^{\mathbb{N}} \\ f = X^n f_0 \end{cases}.$$

4) Soient f et g deux séries formelles à coefficients dans A .

- Si $fg = 0$:

Alors : $v(fg) = v(0) = +\infty \geq v(f) + v(g)$.

- Si $fg \neq 0$:

Posons : $v(f) = n$ et $v(g) = m$.

$fg \neq 0 \Rightarrow [f \neq 0 \text{ et } g \neq 0] \Rightarrow n, m \in \mathbb{N}$.

Il existe alors deux séries formelles f_0 et g_0 à coefficients dans A telles que :

$f = X^n f_0$ et $g = X^m g_0$.

Alors : $fg = (X^n f_0)(X^m g_0) = (X^n X^m)(f_0 g_0) = X^{n+m}(f_0 g_0)$.

Ce qui montre que : $v(fg) \geq n + m = v(f) + v(g)$.

5) Supposons que A est intègre et que f, g sont des séries formelles à coefficients dans A .

a) Supposons que $v(f) = v(g) = 0$.

Posons : $f = (a_k)_{k \in \mathbb{N}}$, $g = (b_k)_{k \in \mathbb{N}}$, $fg = (c_k)_{k \in \mathbb{N}}$.

$v(f) = v(g) = 0 \Rightarrow [a_0 \neq 0 \text{ et } b_0 \neq 0]$.

Puisque A est intègre alors : $c_0 = a_0 b_0 \neq 0 \Rightarrow v(fg) = 0$.

b) - Si $fg = 0$:

Alors : $v(fg) = v(0) = +\infty = v(f) + v(g)$.

- Si $fg \neq 0$:

Posons : $v(f) = n$ et $v(g) = m$.

$fg \neq 0 \Rightarrow [f \neq 0 \text{ et } g \neq 0] \Rightarrow n, m \in \mathbb{N}$.

Il existe alors deux séries formelles f_0 et g_0 à coefficients dans A telles que :

$f = X^n f_0$, $g = X^m g_0$ et $v(f_0) = v(g_0) = 0$.

$$\text{Alors : } \begin{cases} fg = (X^n f_0)(X^m g_0) = (X^n X^m)(f_0 g_0) = X^{n+m}(f_0 g_0) \\ v(f_0 g_0) = 0 \end{cases} .$$

Donc : $v(fg) = n + m = v(f) + v(g)$.

Théorème 1-2-4 :

Si A est un anneau unitaire alors $A^{\mathbb{N}}$ est intègre si et seulement si A est intègre.

Démonstration :

Soit A un anneau unitaire.

$\Rightarrow$) **Si $A^{\mathbb{N}}$ est intègre :**

A est intègre (car A est un sous-anneau de $A^{\mathbb{N}}$).

$\Leftarrow$) **Si A est intègre :**

Soient f et g deux séries formelles à coefficients dans A telles que $fg = 0$.

$$fg = 0 \Rightarrow v(fg) = +\infty \Rightarrow v(f) + v(g) = +\infty \Rightarrow [v(f) = +\infty \text{ ou } v(g) = +\infty]$$

$$\Rightarrow [f = 0 \text{ ou } g = 0].$$

Donc $A^{\mathbb{N}}$ est intègre.

1-3- Dérivée d'une série formelle :

Définition 1-3-1 :

Soit A un anneau unitaire et $f = (a_k)_{k \in \mathbb{N}} \in A^{\mathbb{N}}$ une série formelle à coefficients dans A .

On appelle dérivée de f la série formelle à coefficients dans A notée f' définie par :

$$f' = ((k+1)a_{k+1})_{k \in \mathbb{N}} = (a_1, 2a_2, 3a_3, \dots).$$

Exemple 1-3-2 :

Soit A un anneau unitaire.

$$1) \forall a \in A : a' = 0.$$

$$2) X' = 1.$$

$$3) \forall n \in \mathbb{N}^* : (X^n)' = nX^{n-1}.$$

En effet :

$$1) \forall a \in A : a' = (a\delta_{0,k})'_{k \in \mathbb{N}} = ((k+1)a\delta_{0,k+1})'_{k \in \mathbb{N}} = 0.$$

$$\text{Car on a : } \forall k \in \mathbb{N} : (k+1)a\delta_{0,k+1} = (k+1)a0 = 0.$$

$$2) X' = (\delta_{1,k})'_{k \in \mathbb{N}} = ((k+1)\delta_{1,k+1})'_{k \in \mathbb{N}}.$$

$$\forall k \in \mathbb{N} : \begin{cases} \text{pour } k \neq 0 \text{ on a : } (k+1)\delta_{1,k+1} = (k+1)0 = 0 = \delta_{0,k} \\ \text{pour } k = 0 \text{ on a : } (k+1)\delta_{1,k+1} = \delta_{1,1} = 1 = \delta_{0,0} = \delta_{0,k} \end{cases} .$$

$$\text{Donc : } X' = ((k+1)\delta_{1,k+1})'_{k \in \mathbb{N}} = (\delta_{0,k})'_{k \in \mathbb{N}} = 1.$$

$$3) \forall n \in \mathbb{N}^* : (X^n)' = (\delta_{n,k})'_{k \in \mathbb{N}} = ((k+1)\delta_{n,k+1})'_{k \in \mathbb{N}}.$$

$$\forall k \in \mathbb{N} :$$

- **Pour $k = n - 1$:**

$$(k+1)\delta_{n,k+1} = n\delta_{n,n} = n1 = n\delta_{n-1,n-1} = n\delta_{n-1,k}.$$

- Pour $k \neq n - 1$:

$$(k+1)\delta_{n,k+1} = (k+1)0 = 0 = n0 = n\delta_{n-1,k}.$$

$$\text{Donc : } (X^n)' = ((k+1)\delta_{n,k+1})'_{k \in \mathbb{N}} = (n\delta_{n-1,k})'_{k \in \mathbb{N}} = n(\delta_{n-1,k})'_{k \in \mathbb{N}} = nX^{n-1}.$$

Propriétés 1-3-3 :

Soit A un anneau unitaire .

$$1) \forall f, g \in A^{\mathbb{N}} : (f+g)' = f' + g'.$$

$$2) \forall f, g \in A^{\mathbb{N}} : (fg)' = f'g + fg'.$$

$$3) \forall f \in A^{\mathbb{N}} \quad \text{et} \quad \forall a \in A : \begin{cases} (af)' = a f' \\ (fa)' = f' a \end{cases}.$$

$$4) \forall f \in A^{\mathbb{N}} : ff' = f'f \Rightarrow \forall n \in \mathbb{N}^* : (f^n)' = nf^{n-1} f'.$$

$$5) \text{ Si } A \text{ est abélien alors : } \forall f \in A^{\mathbb{N}} \quad \text{et} \quad \forall n \in \mathbb{N}^* : (f^n)' = nf^{n-1} f'.$$

Démonstration :

1) Soient $f = (a_k)_{k \in \mathbb{N}}$ et $g = (b_k)_{k \in \mathbb{N}}$ deux séries formelles à coefficients dans A .

$$\begin{aligned} (f+g)' &= [(a_k)_{k \in \mathbb{N}} + (b_k)_{k \in \mathbb{N}}]' = (a_k + b_k)'_{k \in \mathbb{N}} = ((k+1)(a_k + b_k))_{k \in \mathbb{N}} \\ &= ((k+1)a_k + (k+1)b_k)_{k \in \mathbb{N}} = ((k+1)a_k)_{k \in \mathbb{N}} + ((k+1)b_k)_{k \in \mathbb{N}} \\ &= (a_k)'_{k \in \mathbb{N}} + (b_k)'_{k \in \mathbb{N}} \\ &= f' + g'. \end{aligned}$$

2) Soient $f = (a_k)_{k \in \mathbb{N}}$ et $g = (b_k)_{k \in \mathbb{N}}$ deux séries formelles à coefficients dans A .

$$\text{Posons } fg = (c_k)_{k \in \mathbb{N}}.$$

$$\forall k \in \mathbb{N} :$$

$$\begin{aligned} (k+1)c_{k+1} &= (k+1) \sum_{j=0}^{k+1} a_j b_{k+1-j} = \sum_{j=0}^{k+1} (k+1) a_j b_{k+1-j} = \sum_{j=0}^{k+1} (j+k+1-j) a_j b_{k+1-j} \\ &= \sum_{j=0}^{k+1} [j a_j b_{k+1-j} + (k+1-j) a_j b_{k+1-j}] \\ &= \sum_{j=0}^{k+1} j a_j b_{k+1-j} + \sum_{j=0}^{k+1} (k+1-j) a_j b_{k+1-j} \\ &= \sum_{j=1}^{k+1} j a_j b_{k+1-j} + \sum_{j=0}^k (k+1-j) a_j b_{k+1-j} \\ &= \sum_{i=0}^k (i+1) a_{i+1} b_{k-i} + \sum_{j=0}^k a_j (k-j+1) b_{k-j+1}. \end{aligned}$$

$$\text{Posons : } f'g = (u_k)_{k \in \mathbb{N}} \quad \text{et} \quad fg' = (v_k)_{k \in \mathbb{N}}.$$

$$\forall k \in \mathbb{N} : u_k = \sum_{i=0}^k (i+1) a_{i+1} b_{k-i} \quad \text{et} \quad v_k = \sum_{j=0}^k a_j (k-j+1) b_{k-j+1}.$$

$$\text{Par suite on a : } (k+1)c_k = u_k + v_k.$$

Ce qui montre que :

$$(fg)' = ((k+1)c_k)_{k \in \mathbb{N}} = (u_k + v_k)_{k \in \mathbb{N}} = (u_k)_{k \in \mathbb{N}} + (v_k)_{k \in \mathbb{N}} = f'g + fg'.$$

3) $\forall f \in A^{\mathbb{N}}$ et $\forall a \in A$:

$$\star (af)' = a'f + af' = 0f + af' = 0 + af' = af'$$

$$\star (fa)' = f'a + fa' = f'a + f0 = f'a + 0 = f'a.$$

4) Soit f une série formelle à coefficients dans A telle que $ff' = f'f$.

Montrons par récurrence que pour tout entier naturel non nul n , $(f^n)' = nf^{n-1}f'$.

- **Pour $n = 1$:**

$$(f^n)' = (f^1)' = f' = 1f^0f' = 1f^{1-1}f' = nf^{n-1}f'$$

- **Pour $n - 1$:**

$$\text{Supposons que } (f^{n-1})' = (n-1)f^{n-2}f'.$$

- **Pour n :**

$$\text{Montrons qu'alors : } (f^n)' = nf^{n-1}f'.$$

$$\begin{aligned} (f^n)' &= (f^{n-1}f)' = (f^{n-1})'f + f^{n-1}f' = [(n-1)f^{n-2}f']f + f^{n-1}f' \\ &= (n-1)f^{n-2}(f'f) + f^{n-1}f' = (n-1)f^{n-2}(ff') + f^{n-1}f' \\ &= (n-1)(f^{n-2}f)f' + f^{n-1}f' = (n-1)(f^{n-1})f' + f^{n-1}f' \\ &= nf^{n-1}f'. \end{aligned}$$

5) Supposons que A est abélien.

Alors $A^{\mathbb{N}}$ est abélien et par suite pour toute série formelle à coefficients dans A on a : $ff' = f'f$.

Ce qui montre que : $\forall f \in A^{\mathbb{N}}$ et $\forall n \in \mathbb{N}^* : (f^n)' = nf^{n-1}f'$.

1-4- Dérivées successives d'une série formelle :

Définition 1-4-1 :

Soit A un anneau unitaire et $f \in A^{\mathbb{N}}$ une série formelle à coefficients dans A .

On définit par récurrence sur $k \in \mathbb{N}$ la dérivée $k^{\text{ième}}$ de f noté $f^{(k)}$ par :

$$\forall k \in \mathbb{N} : \begin{cases} f^{(0)} = f \\ f^{(k)} = [f^{(k-1)}]' \end{cases}$$

- Si $k = 2$, $f^{(2)}$ est appelée la dérivée seconde de f et noté aussi : f'' .

- Si $k = 3$, $f^{(3)}$ est appelée la dérivée tierce de f et noté aussi : f''' .

Exemple 1-4-2 :

Soit A un anneau unitaire .

$$\star \forall a \in A \quad \text{et} \quad \forall k \in \mathbb{N}^* : a^{(k)} = 0.$$

$$\star \begin{cases} X' = 1 \\ \forall k \succ 1 : X^{(k)} = 0 \end{cases}.$$

$$\star \left\{ \begin{array}{l} (X^2)' = 2X \\ (X^2)'' = 2 \\ \forall k \succ 2 : (X^2)^{(k)} = 0 \end{array} \right. .$$

$$\star \left\{ \begin{array}{l} (X^3)' = 3X^2 \\ (X^3)'' = 6X \\ (X^3)''' = 6 \\ \forall k \succ 3 : (X^3)^{(k)} = 0 \end{array} \right. .$$

Propriétés 1-4-3 :

Soit A un anneau unitaire .

- 1) $\forall n, k \in \mathbb{N} : \left\{ \begin{array}{ll} (X^n)^{(k)} = \frac{n!}{(n-k)!} X^{n-k} & \text{si : } k \leq n \\ (X^n)^{(k)} = 0 & \text{si : } k \succ n \end{array} \right. .$
- 2) $\forall f, g \in A^{\mathbb{N}} \text{ et } \forall k \in \mathbb{N} : (f+g)^{(k)} = f^{(k)} + g^{(k)} .$
- 3) $\forall a \in A \text{ et } \forall f \in A^{\mathbb{N}} : (af)^{(k)} = a f^{(k)} .$
- 4) $\forall a \in A \text{ et } \forall f \in A^{\mathbb{N}} : (fa)^{(k)} = f^{(k)} a .$

Démonstration :

1) Montrons par récurrence sur $k \in \mathbb{N}$ que pour tout entier naturel n :

$$\left\{ \begin{array}{ll} (X^n)^{(k)} = \frac{n!}{(n-k)!} X^{n-k} & \text{si : } n \geq k \\ (X^n)^{(k)} = 0 & \text{si : } n < k \end{array} \right. .$$

- **Pour $k = 0$:**

$$\forall n \in \mathbb{N} : (X^n)^{(0)} = (X^n)^{(0)} = X^n = 1X^n = \frac{n!}{n!} X^n = \frac{n!}{(n-0)!} X^{n-0} = \frac{n!}{(n-k)!} X^{n-k} .$$

$$\text{Par suite on a : } \left\{ \begin{array}{ll} (X^n)^{(k)} = \frac{n!}{(n-k)!} X^{n-k} & \text{si : } n \geq 0 = k \\ (X^n)^{(k)} = 0 & \text{si : } n < 0 = k \end{array} \right. .$$

- **Pour $k - 1$:**

$$\text{Supposons que : } \forall n \in \mathbb{N} : \left\{ \begin{array}{ll} (X^n)^{(k-1)} = \frac{n!}{(n-k+1)!} X^{n-k+1} & \text{si : } n \geq k-1 \\ (X^n)^{(k-1)} = 0 & \text{si : } n < k-1 \end{array} \right. .$$

- **Pour k :**

$$\text{Montrons qu'alors : } \forall n \in \mathbb{N} : \left\{ \begin{array}{ll} (X^n)^{(k)} = \frac{n!}{(n-k)!} X^{n-k} & \text{si : } n \geq k \\ (X^n)^{(k)} = 0 & \text{si : } n < k \end{array} \right. .$$

• **Si $n \geq k$:**

Alors $n \geq k - 1$. D'après l'hypothèse de récurrence on a :

$$(X^n)^{(k-1)} = \frac{n!}{(n-k+1)!} X^{n-k+1} .$$

Par suite on a :

$$\begin{aligned}(X^n)^{(k)} &= \left[(X^n)^{(k-1)} \right]' = \left[\frac{n!}{(n-k+1)!} X^{n-k+1} \right]' = \frac{n!}{(n-k+1)!} (X^{n-k+1})' \\&= \frac{n!}{(n-k+1)!} (n-k+1) X^{n-k} \\&= \frac{n!}{(n-k)!} X^{n-k}.\end{aligned}$$

• **Si $n = k - 1$:**

Alors $n = k - 1 \geq k - 1$. D'après l'hypothèse de récurrence on a :

$$\begin{aligned}(X^n)^{(k-1)} &= \frac{n!}{(n-k+1)!} X^{n-k+1} = \frac{(k-1)!}{(k-1-k+1)!} X^{k-1-k+1} = \frac{(k-1)!}{0!} X^0 \\&= \frac{(k-1)!}{1} 1 = (k-1)!.\end{aligned}$$

$$\text{Par suite on a : } (X^n)^{(k)} = \left[(X^n)^{(k-1)} \right]' = [(k-1)!]' = 0.$$

• **Si $n < k - 1$:**

D'après l'hypothèse de récurrence on a : $(X^n)^{(k-1)} = 0$.

$$\text{Par suite on a : } (X^n)^{(k)} = \left[(X^n)^{(k-1)} \right]' = 0' = 0.$$

$$\text{Ce qui montre que : } \forall n, k \in \mathbb{N} : \begin{cases} (X^n)^{(k)} = \frac{n!}{(n-k)!} X^{n-k} & \text{si : } k \leq n \\ (X^n)^{(k)} = 0 & \text{si : } k > n \end{cases}.$$

2) Montrons par récurrence sur $k \in \mathbb{N}$ que si f et g sont des séries formelles à coefficients dans A alors : $(f+g)^{(k)} = f^{(k)} + g^{(k)}$.

- **Pour $k = 0$:**

$$\forall f, g \in A^{\mathbb{N}} : (f+g)^{(k)} = (f+g)^{(0)} = f+g = f^{(0)} + g^{(0)} = f^{(k)} + g^{(k)}.$$

- **Pour $k - 1$:**

$$\text{Supposons que : } \forall f, g \in A^{\mathbb{N}} : (f+g)^{(k-1)} = f^{(k-1)} + g^{(k-1)}.$$

- **Pour k :**

$$\text{Montrons qu'alors : } \forall f, g \in A^{\mathbb{N}} : (f+g)^{(k)} = f^{(k)} + g^{(k)}.$$

$$\begin{aligned}\forall f, g \in A^{\mathbb{N}} : (f+g)^{(k)} &= \left[(f+g)^{(k-1)} \right]' \\&= [f^{(k-1)} + g^{(k-1)}]' \text{ (d'après l'hypothèse de récurrence)} \\&= (f^{(k-1)})' + (g^{(k-1)})' \\&= f^{(k)} + g^{(k)}.\end{aligned}$$

3) Montrons par récurrence sur $k \in \mathbb{N}$ que pour tout élément a de K et pour toute série formelle f à coefficients dans A on a : $(af)^{(k)} = af^{(k)}$.

- **Pour $k = 0$:**

$$\forall a \in K \text{ et } \forall f \in A^{\mathbb{N}} : (af)^{(k)} = (af)^{(0)} = af = af^{(0)} = af^{(k)}.$$

- **Pour $k - 1$:**

$$\text{Supposons que : } \forall a \in K \text{ et } \forall f \in A^{\mathbb{N}} : (af)^{(k-1)} = af^{(k-1)}.$$

- **Pour k :**

$$\text{Montrons qu'alors : } \forall a \in K \text{ et } \forall f \in A^{\mathbb{N}} : (af)^{(k)} = af^{(k)}.$$

$$\forall a \in K \text{ et } \forall f \in A^{\mathbb{N}} :$$

$$\begin{aligned}(af)^{(k)} &= \left[(af)^{(k-1)} \right]' \\&= [af^{(k-1)}]' \text{ (d'après l'hypothèse de récurrence)} \\&= a(f^{(k-1)})' \\&= af^{(k)}.\end{aligned}$$

4) Montrons par récurrence sur $k \in \mathbb{N}$ que pour tout élément a de K et pour toute série formelle f à coefficients dans A on a : $(fa)^{(k)} = f^{(k)}a$.

- **Pour $k = 0$:**

$$\forall a \in K \text{ et } \forall f \in A^{\mathbb{N}} : (fa)^{(0)} = (fa)^{(0)} = fa = f^{(0)}a = f^{(0)}a.$$

- **Pour $k - 1$:**

$$\text{Supposons que : } \forall a \in K \text{ et } \forall f \in A^{\mathbb{N}} : (fa)^{(k-1)} = f^{(k-1)}a.$$

- **Pour k :**

$$\text{Montrons qu'alors : } \forall a \in K \text{ et } \forall f \in A^{\mathbb{N}} : (fa)^{(k)} = f^{(k)}a.$$

$$\forall a \in K \text{ et } \forall f \in A^{\mathbb{N}} :$$

$$\begin{aligned} (fa)^{(k)} &= [(fa)^{(k-1)}]' \\ &= [f^{(k-1)}a]' \text{ (d'après l'hypothèse de récurrence)} \\ &= (f^{(k-1)})'a \\ &= f^{(k)}a. \end{aligned}$$

2-Généralités sur les polynômes :

2-1- Polynômes et degré d'un polynôme :

Définition 2-1-1 :

Soit A un anneau unitaire et $f = (a_k)_{k \in \mathbb{N}} \in A^{\mathbb{N}}$ une série formelle à coefficients dans A .

On dit que f est un polynôme à coefficients dans A ou f est un polynôme s'il existe un entier naturel n tel que : $\forall k \in \mathbb{N} : k > n \Rightarrow a_k = 0$.

Définition 2-1- 2 :

Soit A un anneau unitaire et $f = (a_k)_{k \in \mathbb{N}} \in A^{\mathbb{N}}$ un polynôme à coefficients dans A .

- **Si $f \neq 0$:**

Le plus grand entier naturel k tel que $a_k \neq 0$ est appelé le degré de f et noté $d^0(f)$.

C'est dire : $d^0(f) = \max(\{k \in \mathbb{N} \text{ tq : } a_k \neq 0\})$.

Dans ce cas si $d^0(f) = n$ alors :

★ a_n est appelé le coefficient du plus haut degré de f ou le coefficient dominant de f .

★ Si $a_n = 1$ on dit que le polynôme f unitaire.

- **Si $f = 0$:**

On pose $d^0(0) = -\infty$ appelé le degré de 0.

Exemple 2-1-3 :

Soit A un anneau unitaire.

★ $\forall a \in A^*$:

• a est un polynôme à coefficients dans A et $d^0(a) = 0$.

• a est le coefficient dominant de a .

• a est unitaire si seulement si $a = 1$.

★ $\forall a \in A : a$ est un polynôme à coefficients dans A et $d^0(a) \leq 0$.

★ Les éléments de A sont tous des polynômes à coefficients dans A .

★ X est un polynôme unitaire à coefficients dans A de degré 1 (c'est à dire $d^0(X) = 1$).

★ $\forall n \in \mathbb{N}, X^n$ est un polynôme unitaire à coefficients dans A de degré n .

C'est à dire : $\forall n \in \mathbb{N} : d^0(X^n) = n$.

Propriétés 2-1-4 :

Soit A un anneau unitaire et $f = (a_k)_{k \in \mathbb{N}} \in A^{\mathbb{N}}$ un polynôme à coefficients dans A .

- 1) $d^0(f) \in \mathbb{N} \Leftrightarrow f \neq 0$.
- 2) $d^0(f) = -\infty \Leftrightarrow f = 0$.
- 3) $d^0(f) \in \mathbb{N} \cup \{-\infty\}$.
- 4) $d^0(f) = 0 \Leftrightarrow f \in A^*$.
- 5) $d^0(f) \leq 0 \Leftrightarrow f \in A$.
- 6) $\forall n \in \mathbb{N} : d^0(f) = n \Leftrightarrow \begin{cases} a_n \neq 0 \\ \forall k \in \mathbb{N} : k > n \Rightarrow a_k = 0 \end{cases}$

Dans ce cas a_n est le coefficient dominant de f .

- 7) $\forall n \in \mathbb{N} : d^0(f) \leq n \Leftrightarrow [\forall k \in \mathbb{N} : k > n \Rightarrow a_k = 0]$.

Démonstration :

- 1) $\Rightarrow$) **Si $d^0(f) \in \mathbb{N}$:**

Supposons que $f = 0$.

D'après la définition 2-1-2, $d^0(f) = +\infty \notin \mathbb{N}$. Ce qui est absurde. Donc $f \neq 0$.

- $\Leftarrow$) **Si $f \neq 0$:**

Soit n le plus grand entier naturel k tel que $a_k \neq 0$.

D'après la définition 2-1-2 : $d^0(f) = n \in \mathbb{N}$.

- 2) $\Rightarrow$) **Si $d^0(f) = -\infty$:**

$d^0(f) = -\infty \notin \mathbb{N} \Rightarrow f = 0$ (d'après 1)).

- $\Leftarrow$) **Si $f = 0$:**

D'après la définition 2-1-2) : $d^0(f) = -\infty$.

- 3) - **Si $f \neq 0$:** $d^0(f) \in \mathbb{N} \subset \mathbb{N} \cup \{-\infty\}$.

- **Si $f = 0$:** $d^0(f) = -\infty \in \mathbb{N} \cup \{-\infty\}$.

Donc : $d^0(f) \in \mathbb{N} \cup \{-\infty\}$.

- 4) $\Rightarrow$) **Si $d^0(f) = 0$:**

Alors 0 est le plus grand entier naturel k tel que $a_k \neq 0$.

On a donc : $\begin{cases} a_0 \neq 0 \\ a_k = 0 \quad \forall k > 0 \end{cases}$ Par conséquent on a :

$$\forall k \in \mathbb{N} : \begin{cases} a_k = 0 = a_0 \cdot 0 = a_0 \delta_{0,k} & \text{si } k \neq 0 \\ a_k = a_0 = a_0 \cdot 1 = a_0 \delta_{0,0} = a_0 \delta_{0,k} & \text{si } k = 0 \end{cases}.$$

Ce qui montre que $f = (a_0 \delta_{0,k})_{k \in \mathbb{N}} = a_0 \in A^*$.

- $\Leftarrow$) **Si $f \in A^*$:**

Alors il existe un élément non nul $a \in A^*$ tel que $f = a = (a \delta_{0,k})_{k \in \mathbb{N}}$.

Par suite on a : $\begin{cases} a \delta_{0,0} = a \neq 0 \\ a \delta_{0,k} = 0 \quad \forall k \geq 1 \end{cases} \Rightarrow d^0 f = 0.$

- 5) $d^0(f) \leq 0 \Leftrightarrow [d^0(f) = 0 \text{ ou } d^0(f) < 0] \Leftrightarrow [d^0(f) = 0 \text{ ou } d^0(f) = -\infty]$
 $\Leftrightarrow [f \in A^* \text{ ou } f = 0] \Leftrightarrow f \in A.$

6) Soient n un entier naturel et $I = \{k \in \mathbb{N} \mid a_k \neq 0\}$

$\Rightarrow$) Si $d^0(f) = n$:

Puisque $d^0(f) = n$ est un entier naturel alors f est non nulle et $n = d^0(f)$ est le grand élément de I .

$$\text{On a donc : } \begin{cases} n \in I \\ \forall k \in \mathbb{N} : k > n \Rightarrow k \notin I \end{cases} \Rightarrow \begin{cases} a_n \neq 0 \\ \forall k \in \mathbb{N} : k > n \Rightarrow a_k = 0 \end{cases}.$$

$\Leftarrow$) Si $a_n \neq 0$ et si on a pour tout entier naturel $k > n$, $a_k = 0$:

Posons $d^0(f) = m$.

Puisque $a_n \neq 0$ alors f est non nulle alors $m = d^0(f) \in \mathbb{N}$, m est le plus grand élément de I et $n \in I$.

$$n \in I \Rightarrow m \geq n.$$

Supposons que $m > n$. Alors : $a_m = 0 \Rightarrow d^0(f) = m \notin I$. Ce qui est absurde.

$$\text{Donc } d^0(f) = m = n.$$

Dans ce cas a_n est le coefficient dominant de f .

7) Soient n un entier naturel et posons $d^0(f) = m$.

$\Rightarrow$) Si $d^0(f) \leq n$:

- Si $d^0(f) = -\infty$:

Alors f est nulle. On a donc : $\forall k \in \mathbb{N} : k > n \Rightarrow a_k = 0$.

- Si $d^0(f) \neq -\infty$:

Alors f est non nulle. $\forall k \in \mathbb{N} \mid k > n$.

$$k > n \Rightarrow k > d^0(f) = m \Rightarrow a_k = 0.$$

$\Leftarrow$) Si on a pour tout entier naturel $k > n$, $a_k = 0$:

Posons $d^0(f) = m$ et supposons $m > n$.

Alors $m \in \mathbb{N}$ et $a_m = 0$. Donc $m \neq d^0(f)$. Ce qui est absurde.

$$\text{Ce qui montre que } d^0(f) = m \leq n.$$

Lemme 2-1-5 :

Soient A un anneau unitaire, $f = (a_i)_{i \in \mathbb{N}}$ une série formelle à coefficients dans A et n un entier naturel quelconque.

Les deux propriétés suivantes sont équivalentes :

i) f est un polynôme à coefficients dans A et $d^0(f) \leq n$.

$$\text{ii) } \forall i \in \mathbb{N} : a_i = \sum_{k=0}^n a_k \delta_{k,i}.$$

Dans ce cas : $d^0(f) = n \Leftrightarrow a_n \neq 0$.

Démonstration :

i) $\Rightarrow$ ii) Supposons que f est un polynôme à coefficients dans A et $d^0(f) \leq n$:

Soit i un entier naturel quelconque.

- Si $i \leq n$:

$$\forall k = 0, 1, \dots, n : \begin{cases} a_k \delta_{k,i} = a_k 0 = 0 & \text{si } k \neq i \\ a_k \delta_{k,i} = a_i \delta_{i,i} = a_i 1 = a_i & \text{si } k = i \end{cases}.$$

$$\text{Donc : } a_i = \sum_{k=0}^n a_k \delta_{k,i}.$$

- Si $i > n$:

Alors : $a_i = 0$ (car $i > n \geq d^0(f)$).

$\forall k = 0, 1, \dots, n : k \leq n < i \Rightarrow k \neq i \Rightarrow a_k \delta_{k,i} = a_k 0 = 0$.

Donc : $a_i = 0 = \sum_{k=0}^n a_k \delta_{k,i}$.

ii) $\Rightarrow$ i) Supposons que pour tout entier naturel on a : $a_i = \sum_{k=0}^n a_k \delta_{k,i}$:

Soit i un entier naturel quelconque tel que $i > n$.

$\forall k = 0, 1, \dots, n : k \leq n < i \Rightarrow k \neq i \Rightarrow a_k \delta_{k,i} = a_k 0 = 0$.

Donc : $a_i = 0 = \sum_{k=0}^n a_k \delta_{k,i}$.

Ce qui montre que f est un polynôme à coefficients dans A et $d^0(f) \leq n$.

Dans ce cas :

$\Rightarrow$) Si $d^0(f) = n$:

Alors $a_n \neq 0$ (car a_n est le coefficient dominant de f).

$\Leftarrow$) Si $a_n \neq 0$:

$$\begin{cases} d^0(f) \leq n \\ a_n \neq 0 \end{cases} \Rightarrow \begin{cases} d^0(f) \leq n \\ n \leq d^0(f) \end{cases} \Rightarrow d^0(f) = n$$

Théorème 2-1-6 :

Soient A un anneau unitaire , $f = (a_i)_{i \in \mathbb{N}}$ une série formelle à coefficients dans A et n un entier naturel quelconque.

Les deux propriétés suivantes sont équivalentes :

i) f est un polynôme à coefficients dans A et $d^0(f) \leq n$.

ii) $f = \sum_{k=0}^n a_k X^k = a_0 + a_1 X + a_2 X^2 + \dots + a_n X^n$.

Dans ce cas : $d^0(f) = n \Leftrightarrow a_n \neq 0$.

Démonstration :

$[f \text{ est un polynôme à coefficients dans } A \text{ et } d^0(f) \leq n]$ (d'après le lemme 2-1-5)

$$\Leftrightarrow \left[\forall i \in \mathbb{N} : a_i = \sum_{k=0}^n a_k \delta_{k,i} \right]$$

$$\Leftrightarrow \left[f = \left(\sum_{k=0}^n a_k \delta_{k,i} \right)_{i \in \mathbb{N}} \right] \Leftrightarrow \left[f = \sum_{k=0}^n (a_k \delta_{k,i})_{i \in \mathbb{N}} \right]$$

$$\Leftrightarrow f = \sum_{k=0}^n a_k X^k.$$

Dans ce cas : $d^0(f) = n \Leftrightarrow a_n \neq 0$ (d'après le lemme 2-1-5).

Théorème 2-1-7 :

Soit A un anneau unitaire, $f = (\alpha_i)_{i \in \mathbb{N}}$ une série formelle à coefficients dans A et $a_0, a_1, \dots, a_n$ des éléments quelconque de A .

$$f = \sum_{k=0}^n a_k X^k \Leftrightarrow \forall i \in \mathbb{N} : \begin{cases} \alpha_i = a_i & \text{si } i \leq n \\ \alpha_i = 0 & \text{si } i > n \end{cases}$$

Dans ce cas :

1) f est un polynôme à coefficients dans A et $d^0(f) \leq n$.

2) $d^0(f) = n \Leftrightarrow a_n \neq 0 \Leftrightarrow \alpha_n \neq 0$.

Démonstration :

$$\Rightarrow) \text{ Si } f = \sum_{k=0}^n a_k X^k :$$

$$\text{Alors : } (\alpha_i)_{i \in \mathbb{N}} = f = \sum_{k=0}^n a_k X^k = \sum_{k=0}^n a_k (\delta_{k,i})_{i \in \mathbb{N}} = \sum_{k=0}^n (a_k \delta_{k,i})_{i \in \mathbb{N}} = \left(\sum_{k=0}^n a_k \delta_{k,i} \right)_{i \in \mathbb{N}}.$$

$$\text{Par suite on a : } \forall i \in \mathbb{N} : \begin{cases} \alpha_i = \sum_{k=0}^n a_k \delta_{k,i} = a_i & \text{si } i \leq n \\ \alpha_i = \sum_{k=0}^n a_k \delta_{k,i} = 0 & \text{si } i > n \end{cases}.$$

$\Rightarrow)$ **Si pour tout entier naturel $i \leq n$, $\alpha_i = a_i$ et pour tout entier $i > n$, $\alpha_i = 0$:**

Puisque f est un polynôme et puisque $d^0(f) \leq n$ (car $\alpha_i = 0$ pour tout entier $i > n$)

$$\text{alors (d'après le théorème 2-1-6) : } f = \sum_{k=0}^n \alpha_k X^k = \sum_{k=0}^n a_k X^k.$$

Dans ce cas (d'après le lemme 2-1-5) :

1) f est un polynôme à coefficients dans A et $d^0(f) \leq n$.

2) $d^0(f) = n \Leftrightarrow \alpha_n \neq 0 \Leftrightarrow a_n \neq 0$.

Corollaire 2-1-8 :

Soit A un anneau unitaire, f est un polynôme à coefficients dans A et n un entier naturel quelconque.

Si $d^0(f) \leq n$, il existe d'une façon unique $a_0, a_1, \dots, a_n \in A$ tels que :

$$f = \sum_{k=0}^n \alpha_k X^k = a_0 + a_1 X + a_2 X^2 + \dots + a_n X^n.$$

Démonstration :

Posons $f = (\alpha_i)_{i \in \mathbb{N}}$.

- **Existence :**

Puisque f est un polynôme et puisque $d^0(f) \leq n$ alors (d'après le théorème 2-1-6) :

$$f = \sum_{k=0}^n a_k X^k.$$

D'où l'existence.

- Unicité :

Soient $\alpha_0, \alpha_1, \dots, \alpha_n$ des éléments quelconque de A tels que $f = \sum_{k=0}^n \alpha_k X^k$.

D'après le théorème 2-1-7 on a : $\forall k = 0, 1, \dots, n : \alpha_k = a_k$.

D'où l'unicité.

Corollaire 2-1-9 :

Soit A un anneau unitaire, f est un polynôme à coefficients dans A et n un entier naturel quelconque.

Si $d^0(f) = n$ il existe d'une façon unique des éléments $a_0, a_1, \dots, a_n \in A$ tels que :

$$f = \sum_{k=0}^n a_k X^k = a_0 + a_1 X + a_2 X^2 + \dots + a_n X^n \quad \text{et} \quad a_n \neq 0.$$

a_n est le coefficient dominant de f .

En effet :

Supposons que $d^0(f) = n$.

Puisque $d^0(f) = n \leq n$ alors d'après le corollaire 2-1-8, il existe d'une façon unique

$$a_0, a_1, \dots, a_n \in A \text{ tels que : } f = \sum_{k=0}^n \alpha_k X^k.$$

Comme on a $d^0(f) = n$ alors $a_n \neq 0$. Donc a_n est le coefficient dominant de f .

Corollaire 2-1-10 :

Soit A un anneau unitaire .

Pour tout polynôme f à coefficients dans A il existent des éléments

$$a_0, a_1, \dots, a_n \in A \text{ tels que : } f = \sum_{k=0}^n \alpha_k X^k = a_0 + a_1 X + a_2 X^2 + \dots + a_n X^n.$$

En effet :

Soit $f = (a_i)_{i \in \mathbb{N}}$ un polynôme à coefficients dans A .

Il existe un entier naturel n tel que : $\forall k \in \mathbb{N} : k > n \Rightarrow \alpha_k = 0$.

D'après la propriété 2-1-4 7), $d^0(f) \leq n$ par suite il existe (d'après le corollaire 2-1-8)

$$a_0, a_1, \dots, a_n \in A \text{ tels que : } f = \sum_{k=0}^n \alpha_k X^k.$$

Corollaire 2-1-11 :

Soit A un anneau unitaire .

Si f et g sont deux polynômes à coefficients dans A alors il existe des éléments

$a_0, a_1, \dots, a_n, b_0, b_1, \dots, b_n \in A$ tels que :

$$f = \sum_{k=0}^n \alpha_k X^k \quad \text{et} \quad g = \sum_{k=0}^n b_k X^k.$$

En effet :

Soient $f = (a_k)_{k \in \mathbb{N}}$ et $g = (b_k)_{k \in \mathbb{N}}$ deux polynômes à coefficients dans A .

Il existe deux entiers naturels n_1 et n_2 tels que : $\forall k \in \mathbb{N} : \begin{cases} k > n_1 \Rightarrow a_k = 0 \\ k > n_2 \Rightarrow b_k = 0 \end{cases}$.

Posons $n = \max(n_1, n_2)$, on a alors pour tout entier naturel $k > n$, $a_k = b_k = 0$.

D'après la propriété 2-1-4 7), $d^0(f) \leq n$. Par suite (d'après le théorème 2-1-6) on a :

$$f = \sum_{k=0}^n a_k X^k \quad \text{et} \quad g = \sum_{k=0}^n b_k X^k.$$

Corollaire 2-1-12 :

Soient A un anneau unitaire et $a_0, a_1, \dots, a_n$ des éléments quelconque de A .

La série formelle $f = \sum_{k=0}^n a_k X^k$ à coefficients dans A est un polynôme et $d^0 f \leq n$.

Si de plus $a_n \neq 0$, f est non nul de degré n et de coefficient dominant a_n .

Démonstration :

Posons $f = \sum_{k=0}^n a_k X^k = (\alpha_i)_{i \in \mathbb{N}}$.

D'après le théorème 2-1-7, $f = \sum_{k=0}^n a_k X^k$ est un polynôme et $d^0 f \leq n$.

Si de plus $a_n \neq 0$ alors (d'après le théorème 2-1-7) f est non nul de degré n et de coefficient dominant a_n .

Corollaire 2-1-13 :

Soient A un anneau unitaire et $a_0, a_1, \dots, a_n, b_0, b_1, \dots, b_n$ des éléments quelconques de A .

Si $\sum_{k=0}^n a_k X^k = \sum_{k=0}^n b_k X^k$ alors pour tout entier naturel $k \leq n$, $a_k = b_k$.

C'est à dire : $\sum_{k=0}^n a_k X^k = \sum_{k=0}^n b_k X^k \Rightarrow \forall k = 0, 1, \dots, n : a_k = b_k$.

En effet :

Posons $f = \sum_{k=0}^n a_k X^k$ et supposons que $f = \sum_{k=0}^n a_k X^k = \sum_{k=0}^n b_k X^k$.

D'après le corollaire 2-1-12 $f = \sum_{k=0}^n a_k X^k$ est un polynôme et $d^0 f \leq n$.

Puisque f est un polynôme, $d^0 f \leq n$ et $f = \sum_{k=0}^n a_k X^k = \sum_{k=0}^n b_k X^k$ alors, d'après le

corollaire 2-1-8, $a_k = b_k$ pour tout entier naturel $k \leq n$.

Corollaire 2-1-14 :

Soient A anneau unitaire et $a_0, a_1, \dots, a_n$ des éléments quelconques de A .

Si $\sum_{k=0}^n a_k X^k = 0$ alors, pour tout entier naturel $k \leq n$, $a_k = 0$.

C'est à dire : $\sum_{k=0}^n a_k X^k = 0 \Rightarrow a_0 = a_1 = \dots = a_n = 0$.

En effet :

Supposons que $\sum_{k=0}^n a_k X^k = 0$.

Alors : $\sum_{k=0}^n a_k X^k = \sum_{k=0}^n 0 X^k \Rightarrow \forall k = 0, 1, \dots, n : a_k = 0$ (d'après le corollaire 2-1-13).

Notation 2-1-15 :

Soit A anneau unitaire.

★ L'ensemble des polynômes à coefficients dans A est noté $A[X]$.

★ Pour tout entier naturel n on note par $A_n[X]$ l'ensemble :

$$A_n[X] = \{f \in A[X] \quad tq : d^0(f) \leq n\}$$

Propriétés 2-1-16 :

Soit A un anneau unitaire.

- 1) Pour tout entier naturel n , $A \subset A_n[X] \subset A[X]$.
- 2) Si B est un sous-anneau unitaire de A alors :
 - a) $B[X] \subset A[X]$.
 - b) Pour tout entier naturel n , $B_n[X] \subset A_n[X]$.
- 3) $\mathbb{Z}[X] \subset \mathbb{Q}[X] \subset \mathbb{R}[X] \subset \mathbb{C}[X]$.
- 4) Pour tout entier naturel n , $\mathbb{Z}_n[X] \subset \mathbb{Q}_n[X] \subset \mathbb{R}_n[X] \subset \mathbb{C}_n[X]$.
- 5) Si $A = \mathbb{C}$ alors : $\forall f \in \mathbb{C}[X] : f \in \mathbb{R}[X] \Leftrightarrow \bar{f} = f$.
- 6) Pour tout entier naturel n , $A_n[X]$ est un sous-groupe de $(A^{\mathbb{N}}, +)$.
- 7) $A[X]$ est un sous-groupe de $(A^{\mathbb{N}}, +)$ contenant A et X .
- 8) Soient f et g deux polynômes à coefficients dans A .
 - a) $d^0(f+g) \leq \max(d^0(f), d^0(g))$.
 - b) Si $d^0(f) \neq d^0(g)$ alors : $d^0(f+g) = \max(d^0(f), d^0(g))$.
 - c) Soient n et m deux entiers naturels.

Si $\begin{cases} f \in A_n[X], \text{ dont le coefficient de degré } n \text{ est } \alpha \\ g \in A_m[X], \text{ dont le coefficient de degré } m \text{ est } \beta \end{cases}$

alors $fg \in A_{n+m}[X]$ dont le coefficient de degré $n+m$ est $\alpha\beta$.
 - d) $fg \in A[X]$ et $d^0(fg) \leq d^0(f) + d^0(g)$.
 - e) Si f et g sont non nuls de coefficient dominants respectivement α et β et si $\alpha\beta$ est non nul alors : $d^0(fg) = d^0(f) + d^0(g)$ et fg est non nul de coefficient dominant $\alpha\beta$.
 - f) Si f et g sont non nuls de coefficient dominants respectivement α et β et si l'un des éléments α et β est inversible alors $d^0(fg) = d^0(f) + d^0(g)$ et fg est non nul de coefficient dominant $\alpha\beta$.

- g) Si f et g sont unitaires alors fg est unitaire et $d^0(fg) = d^0(f) + d^0(g)$.
- h) Si A est intègre, f est non nul de coefficient dominant α et g est non nul de coefficient dominant β alors : $d^0(fg) = d^0(f) + d^0(g)$ et fg est non nul de coefficient dominant $\alpha\beta$.
- i) Si A est intègre alors : $d^0(fg) = d^0(f) + d^0(g)$.
- 9) $A[X]$ est un sous-anneau unitaire de $A^{\mathbb{N}}$ contenant A et X .
- 10) $A[X]$ est le petit (pour l'inclusion) sous-anneau de $A^{\mathbb{N}}$ contenant A et X .
- 11) $A[X]$ est nul si et seulement si A est nul. C'est à dire : $A[X] \neq 0 \Leftrightarrow A \neq 0$.
- 12) $A[X]$ n'est pas un corps.
- 13) $A[X]$ est abélien si et seulement si A est abélien.
- 14) $A[X]$ est intègre si et seulement si A est intègre.
- 15) Si A est intègre alors : $U(A[X]) = U(A)$.

Démonstration :

1) Soit n un entier naturel quelconque.

★ $\forall a \in A$: a est polynôme à coefficients dans A et $d^0 a \leq 0 \leq n$. Donc $a \in A_n[X]$.

Ce qui prouve que $A \subset A_n[X]$.

★ $\forall f \in A_n[X] : \exists a_0, a_1, \dots, a_n \in A$ tq : $f = \sum_{k=0}^n a_k X^k$. Donc : $f \in A[X]$.

Ce qui prouve que $A_n[X] \subset A[X]$.

Par conséquent on a : $A \subset A_n[X] \subset A[X]$

2) Supposons que B est un sous-anneau unitaire de A .

a) $\forall f \in B[X] : \exists a_0, a_1, \dots, a_n \in B$ tq : $f = \sum_{k=0}^n a_k X^k$.

$$a_0, a_1, \dots, a_n \in B \subset A \Rightarrow f = \sum_{k=0}^n a_k X^k \in A[X].$$

Donc : $B[X] \subset A[X]$.

b) $\forall n \in \mathbb{N}$ et $\forall f \in B_n[X] : \exists a_0, a_1, \dots, a_n \in B$ tq : $f = \sum_{k=0}^n a_k X^k$.

$$a_0, a_1, \dots, a_n \in B \subset A \Rightarrow f = \sum_{k=0}^n a_k X^k \in A_n[X].$$

Donc : $B_n[X] \subset A_n[X]$.

3) $\mathbb{Z}[X] \subset \mathbb{Q}[X] \subset \mathbb{R}[X] \subset \mathbb{C}[X]$.

Car $\mathbb{Z}$ est un sous-anneau unitaire de $\mathbb{Q}$, $\mathbb{Q}$ est un sous-anneau unitaire de $\mathbb{R}$ et $\mathbb{R}$ est un sous-anneau unitaire de $\mathbb{C}$.

4) $\forall n \in \mathbb{N} : \mathbb{Z}_n[X] \subset \mathbb{Q}_n[X] \subset \mathbb{R}_n[X] \subset \mathbb{C}_n[X]$.

Car $\mathbb{Z}$ est un sous-anneau unitaire de $\mathbb{Q}$, $\mathbb{Q}$ est un sous-anneau unitaire de $\mathbb{R}$ et $\mathbb{R}$ est un sous-anneau unitaire de $\mathbb{C}$.

5) Supposons que $A = \mathbb{C}$ et soit f un polynôme à coefficients complexes.

$\Rightarrow$ Si $f \in \mathbb{R}[X]$:

Alors : $f \in \mathbb{R}[X] \subset \mathbb{R}^{\mathbb{N}} \Rightarrow \bar{f} = f$.

$\Leftrightarrow$ Si $\bar{f} = f$:

Posons $f = (a_k)_{k \in \mathbb{N}}$. $f \in \mathbb{C}[X] \Rightarrow \exists n \in \mathbb{N} \text{ tq : } \forall k \succ n : a_k = 0$.

$$\begin{cases} f \in \mathbb{C}[X] \subset \mathbb{C}^{\mathbb{N}} \\ \bar{f} = f \end{cases} \Rightarrow f \in \mathbb{R}^{\mathbb{N}}.$$

Puisque $f \in \mathbb{R}^{\mathbb{N}}$ et puisqu'on a $a_k = 0$ pour tout entier naturel $k \succ n$ alors $k \succ n$.

6) Soit n un entier naturel quelconque.

★ Puisque $A_n[X]$ contient A et puisque A est non vide alors $A_n[X]$ est non vide.

★ $\forall f, g \in A_n[X] : \exists a_0, a_1, \dots, a_n, b_0, b_1, \dots, b_n \in A \text{ tq :}$

$$f = \sum_{k=0}^n a_k X^k \quad \text{et} \quad g = \sum_{k=0}^n b_k X^k.$$

$$\text{Alors : } f - g = \sum_{k=0}^n a_k X^k - \sum_{k=0}^n b_k X^k = \sum_{k=0}^n (a_k X^k - b_k X^k) = \sum_{k=0}^n (a_k - b_k) X^k \in A_n[X].$$

Donc $A_n[X]$ est un sous-groupe de $(A^{\mathbb{N}}, +)$.

7) ★ $A[X]$ contient A et X (d'après 1) et l'exemple 2-1-3).

★ Puisque $A_n[X]$ contient X alors $A_n[X]$ est non vide.

★ $\forall f, g \in A[X] : \exists a_0, a_1, \dots, a_n, b_0, b_1, \dots, b_n \in A \text{ tq :}$

$$f = \sum_{k=0}^n a_k X^k \quad \text{et} \quad g = \sum_{k=0}^n b_k X^k.$$

Alors : $f, g \in A_n[X] \Rightarrow f - g \in A_n[X] \subset A[X]$.

Donc $A[X]$ est un sous-groupe de $(A^{\mathbb{N}}, +)$ contenant A et X .

8) Soit $f, g \in A[X] :$

a) Posons $\max(d^0(f), d^0(g)) = n$.

- Si $n = -\infty$:

$\max(d^0(f), d^0(g)) = n = -\infty \Rightarrow d^0(f) = d^0(g) = -\infty \Rightarrow f = g = 0$. On a donc :
 $d^0(f+g) = d^0(0+0) = d^0(0) = -\infty = \max(d^0(f), d^0(g)) \leq \max(d^0(f), d^0(g))$.

- Si $n \neq -\infty$:

$$\text{Alors : } n \in \mathbb{N}. \begin{cases} d^0(f) \leq \max(d^0(f), d^0(g)) = n \\ d^0(g) \leq \max(d^0(f), d^0(g)) = n \end{cases} \Rightarrow \begin{cases} f \in A_n[X] \\ g \in A_n[X] \end{cases} \Rightarrow f+g \in A_n[X].$$

Donc : $d^0(f+g) \leq n = \max(d^0(f), d^0(g))$.

b) Supposons que $d^0(f) \neq d^0(g)$ et posons $\max(d^0(f), d^0(g)) = n$.

$d^0(f) \neq d^0(g) \Rightarrow [d^0(f) \neq -\infty \text{ ou } d^0(g) \neq -\infty] \Rightarrow n = \max(d^0(f), d^0(g)) \in \mathbb{N}$.

$$\begin{cases} d^0(f) \leq \max(d^0(f), d^0(g)) = n \\ d^0(g) \leq \max(d^0(f), d^0(g)) = n \end{cases} \Rightarrow \begin{cases} f \in A_n[X] \\ g \in A_n[X] \end{cases}.$$

$$\text{Alors : } \exists a_0, a_1, \dots, a_n, b_0, b_1, \dots, b_n \in A \text{ tq : } f = \sum_{k=0}^n a_k X^k \quad \text{et} \quad g = \sum_{k=0}^n b_k X^k.$$

$$\text{Par suite on a : } f+g = \sum_{k=0}^n a_k X^k + \sum_{k=0}^n b_k X^k = \sum_{k=0}^n (a_k X^k + b_k X^k) = \sum_{k=0}^n (a_k + b_k) X^k.$$

$d^0(f) \neq d^0(g) \Rightarrow [n = d^0(f) \succ d^0(g) \text{ ou } d^0(f) < d^0(g) = n]$.

- Si $n = d^0(f) \succ d^0(g)$:

$$[a_n \neq 0 \text{ et } b_n = 0] \Rightarrow a_n + b_n = a_n + 0 = a_n \neq 0.$$

- Si $d^0(f) < d^0(g) = n$:

$$[a_n = 0 \text{ et } b_n \neq 0] \Rightarrow a_n + b_n = 0 + b_n = b_n \neq 0.$$

Ce qui montre que : $d^0(f+g) = n = \max(d^0(f), d^0(g))$.

c) Supposons que $\begin{cases} f \in A_n[X], \text{ dont le coefficient de degré } n \text{ est } \alpha \\ g \in A_m[X], \text{ dont le coefficient de degré } m \text{ est } \beta \end{cases}$.

Posons : $f = (a_k)_{k \in \mathbb{N}}$, $g = (b_k)_{k \in \mathbb{N}}$ et $fg = (c_k)_{k \in \mathbb{N}}$.

$$f \in A_n[X] \Rightarrow [\forall k \in \mathbb{N} : k > n \Rightarrow a_k = 0].$$

$$g \in A_m[X] \Rightarrow [\forall k \in \mathbb{N} : k > m \Rightarrow b_k = 0].$$

★ Soit k un entier naturel quelconque tel que $k > n + m$. $c_k = \sum_{i=0}^k a_i b_{k-i}$.

$$\forall i = 0, 1, \dots, k :$$

- Si $i > n$:

$$\text{Alors : } a_i = 0 \Rightarrow a_i b_{k-i} = 0.$$

- Si $i \leq n$:

$$\text{Alors : } -i \geq -n \Rightarrow k - i \geq k - n > n + m - n = m.$$

$$\text{Donc : } b_{k-i} = 0 \Rightarrow a_i b_{k-i} = 0.$$

$$\text{Par suite : } c_k = \sum_{i=0}^k a_i b_{k-i} = 0.$$

Ce qui montre que $fg \in A_{n+m}[X]$.

★ $a_n = \alpha$ et $b_m = \beta$. c_{n+m} est le coefficient de fg de degré $n + m$.

$$c_{n+m} = \sum_{i=0}^k a_i b_{n+m-i}.$$

$$\forall i = 0, 1, \dots, n + m :$$

- Si $i > n$:

$$\text{Alors : } a_i = 0 \Rightarrow a_i b_{n+m-i} = 0.$$

- Si $i \leq n$:

$$\text{Alors : } -i > -n \Rightarrow n + m - i > n + m - n = m.$$

$$\text{Donc : } b_{n+m-i} = 0 \Rightarrow a_i b_{n+m-i} = 0.$$

$$\text{Par suite : } c_{n+m} = \sum_{i=0}^k a_i b_{n+m-i} = a_n b_m = \alpha \beta.$$

d) - Si $fg = 0$:

$$\text{Alors : } fg = 0 \in A[X] \text{ et } d^0(fg) = d^0(0) = -\infty \leq d^0(f) + d^0(g).$$

- Si $fg \neq 0$:

$$\text{Posons : } d^0(f) = n \text{ et } d^0(g) = m.$$

$$fg \neq 0 \Rightarrow [f \neq 0 \text{ et } g \neq 0] \Rightarrow [n = d^0(f) \in \mathbb{N} \text{ et } m = d^0(g) \in \mathbb{N}].$$

$$\text{Par suite } f \in A_n[X] \text{ et } g \in A_m[X].$$

$$\text{D'après c) } fg \in A_{n+m}[X] \subset A[X].$$

$$fg \in A_{n+m}[X] \Rightarrow d^0(fg) \leq n + m = d^0(f) + d^0(g).$$

e) Supposons que f et g sont non nuls de coefficients dominants respectivement α et β et que $\alpha\beta$ est non nul.

$$\text{Posons } d^0(f) = n \text{ et } d^0(g) = m.$$

Puisque f et g sont non nuls alors n et m sont des entiers naturels.

Par suite $f \in A_n[X]$, $g \in A_m[X]$, α est le coefficient de f de degré n et β est le coefficient de g de degré m .

D'après c), $fg \in A_{n+m}[X]$ et $\alpha\beta$ est le coefficient de fg de degré $n + m$.

Alors : $d^0(fg) \leq n + m = d^0(f) + d^0(g)$.

$$\begin{cases} d^0(fg) \leq n + m \\ \alpha\beta \text{ est le coefficient de } fg \text{ de degré } n + m \\ \alpha\beta \neq 0 \end{cases}$$

Ce qui montre que fg est non nul, $d^0(fg) = n + m = d^0(f) + d^0(g)$ et $\alpha\beta$ est le coefficient dominant de fg .

f) Supposons que f et g sont non nuls de coefficient dominants respectivement α et β et que l'un des éléments α et β est inversible.

Puisque α et β sont non nuls et l'un des deux au moins est inversible alors, d'après e), on a : $d^0(fg) = d^0(f) + d^0(g)$ et fg est non nul de coefficient dominant $\alpha\beta$.

g) Supposons que f et g sont unitaires.

Alors f et g sont non nuls de coefficient dominants inversibles.

Donc (d'après f)) : $d^0(fg) = d^0(f) + d^0(g)$ et fg est non nul de coefficient dominant $1 \times 1 = 1$.

Ce qui montre que fg est unitaire et que $d^0(fg) = d^0(f) + d^0(g)$.

h) Supposons que A est intègre, f est non nul de coefficient dominant α et g est non nul de coefficient dominant β .

Puisque A est intègre et puisque α et β sont non nuls alors $\alpha\beta$ est non nul.

Donc (d'après e)) : $d^0(fg) = d^0(f) + d^0(g)$ et fg est non nul de coefficient dominant $\alpha\beta$.

i) Supposons que A est intègre.

- Si $f = 0$ ou $g = 0$:

Alors : $[d^0(f) = -\infty \text{ ou } d^0(g) = -\infty] \Rightarrow d^0(f) + d^0(g) = -\infty$.

Donc : $d^0(fg) = d^0(0) = -\infty = d^0(f) + d^0(g)$.

- Si $f \neq 0$ et $g \neq 0$:

D'après h) on a alors : $d^0(fg) = d^0(f) + d^0(g)$.

9) ★ D'après 7), $A[X]$ est un sous-groupe de $(A^{\mathbb{N}}, +)$ contenant A et X .

★ D'après 8) d)), on a : $\forall f, g \in A[X] : fg \in A[X]$.

★ D'après 1)), on a : $1 \in A \subset A[X]$.

Donc $A[X]$ est un sous-anneau unitaire de $A^{\mathbb{N}}$ contenant A et X .

10) Soit B un sous-anneau quelconque de $A^{\mathbb{N}}$ contenant A et X .

$$\forall f \in A[X] : \exists a_0, a_1, \dots, a_n \in A \text{ tq : } f = \sum_{k=0}^n a_k X^k.$$

$$\text{Puisque } B \text{ contenant } A \text{ et } X \text{ alors : } f = \sum_{k=0}^n a_k X^k \in B.$$

Donc : $A[X] \subset B$.

Ce qui montre que $A[X]$ est le petit (pour l'inclusion) sous-anneau de $A^{\mathbb{N}}$ contenant A et X .

11) $\Rightarrow$) Si $A[X]$ est nul :

Alors A est nul (car A est un sous-anneau de $A[X]$).

$\Leftarrow$) Si A est nul :

Alors $A^{\mathbb{N}}$ est nul. Donc $A[X]$ est nul (car $A[X]$ est un sous-anneau de $A^{\mathbb{N}}$).

12) - Si A est nul :

Alors (d'après 11)), $A[X]$ est nul. Donc $A[X]$ n'est pas un corps.

- Si A est non nul :

D'après la propriété 1-1-5-7), X est un élément non nul et non inversible de $A^{\mathbb{N}}$.

Par suite X est un élément non nul et non inversible de $A[X]$.

Donc $A[X]$ n'est pas un corps.

13) - Si $A[X]$ est abélien :

Alors A est abélien (car A est un sous-anneau de $A[X]$).

- Si A est abélien :

D'après la propriété 1-1-5-2), $A^{\mathbb{N}}$ est abélien.

Donc $A[X]$ est abélien (car $A[X]$ est un sous-anneau de $A^{\mathbb{N}}$).

14) - Si $A[X]$ est intègre :

Alors A est intègre (car A est un sous-anneau de $A[X]$).

- Si A est intègre :

D'après le théorème 1-2-4), $A^{\mathbb{N}}$ est intègre.

Donc $A[X]$ est intègre (car $A[X]$ est un sous-anneau de $A^{\mathbb{N}}$).

15) Supposons que A est intègre.

$$\star \forall a \in U(A) : [a^{-1} \in A \subset A[X] \text{ et } aa^{-1} = a^{-1}a = 1] \Rightarrow a \in U(A[X]).$$

Donc : $U(A) \subset U(A[X])$.

$$\star \forall u \in U(A[X]) : uu^{-1} = 1 \Rightarrow d^0u + d^0(u^{-1}) = d^0(uu^{-1}) = d^0(1) = 0.$$

Alors : $d^0u = d^0(u^{-1}) = 0 \Rightarrow u, u^{-1} \in A \Rightarrow u \in U(A)$.

Donc : $U(A[X]) \subset U(A)$.

Ce qui montre que $U(A[X]) = U(A)$.

Contre exemple 2-1-17 :

Si $A = \mathbb{Z}/4\mathbb{Z}$ et $f = \overline{2}X + \overline{1}$ alors :

$$ff = f^2 = (\overline{2}X + \overline{1})^2 = \overline{1} \Rightarrow f \in U([X]) - U(A).$$

Donc $U(A[X]) \neq U(A)$.

Remarque 2-1-18 :

Soit A un anneau unitaire.

1) Pour tout entier naturel n , $A_n[X]$ est un sous groupe de $(A[X], +)$.

Car $A_n[X]$ et $A[X]$ sont des sous-groupes de $(A^{\mathbb{N}}, +)$ et $A_n[X] \subset A[X]$.

2) $\forall \alpha \in A$, $\forall n \in \mathbb{N}$ et $\forall f \in A_n[X] : \alpha f, f\alpha \in A_n[X]$.

Car : $\forall \alpha \in A$, $\forall n \in \mathbb{N}$ et $\forall f \in A_n[X] :$

$$\begin{cases} d^0(\alpha f) \leq d^0(\alpha) + d^0(f) \leq 0 + d^0(f) = d^0(f) \leq n \\ d^0(f\alpha) \leq d^0(f) + d^0(\alpha) \leq d^0(f) + 0 = d^0(f) \leq n \end{cases} . \text{ Donc } \alpha f, f\alpha \in A_n[X].$$

Propriétés 2-1-19 :

Soit A un anneau unitaire.

1) Pour tout entier naturel n , l'application suivante : $\varphi_n : A^{n+1} \rightarrow A_n[X]$

$$a = (a_0, a_1, \dots, a_n) \mapsto \varphi_n(a) = \sum_{k=0}^n a_k X^k$$

est un isomorphisme du groupe additif $(A^{n+1}, +)$ vers le groupe additif $(A_n[X], +)$.

2) Pour tout entier naturel n , $(A_n[X], +)$ est isomorphe à $(A^{n+1}, +)$.

C'est à dire : $\forall n \in \mathbb{N} : (A_n[X], +) \simeq (A^{n+1}, +)$

3) Pour tout entier naturel n , $A_n[X]$ est d'ordre fini si et seulement si A est d'ordre fini et dans ce cas : $|A_n[X]| = |A|^{n+1}$.

4) Si $f = \sum_{i=0}^n \alpha_i X^i$ est un polynôme à coefficients dans A et si $n \geq 1$ alors :

$$a) f' = \sum_{i=1}^n i \alpha_i X^{i-1} = \sum_{k=0}^{n-1} (k+1) \alpha_{k+1} X^k = a_1 + 2a_2 X + 3a_3 X^2 + \dots + n \alpha_n X^{n-1} \in A[X].$$

b) Pour tout entier naturel k ,

$$\begin{cases} f^{(k)} = \sum_{i=k}^n \frac{i! \alpha_i}{(i-k)!} X^{i-k} = \sum_{j=0}^{n-k} \frac{(j+k)! \alpha_{j+k}}{j!} X^j & \text{si : } k \leq n \\ f^{(k)} = 0 & \text{si : } k > n \end{cases}.$$

c) Pour tout entier naturel k , $f^{(k)} \in A[X]$.

d) Pour tout entier naturel $k = 0, 1, \dots, n$, $k! \alpha_k$ est le coefficient constant de $f^{(k)}$.

e) $f^{(n)} = n! \alpha_n$.

Démonstration :

1) Soient n un entier naturel quelconque.

★ $\forall a = (a_0, a_1, \dots, a_n) \in A^{n+1}$ et $\forall b = (b_0, b_1, \dots, b_n) \in A^{n+1}$:

$$\begin{aligned} \varphi_n(a+b) &= \varphi_n((a_0+b_0, a_1+b_1, \dots, a_n+b_n)) = \sum_{k=0}^n (\alpha_k + b_k) X^k \\ &= \sum_{k=0}^n (\alpha_k X^k + b_k X^k) = \sum_{k=0}^n \alpha_k X^k + \sum_{k=0}^n b_k X^k \\ &= \varphi_n(a) + \varphi_n(b). \end{aligned}$$

Donc φ_n est un homomorphisme du groupe additif $(A^{n+1}, +)$ vers le groupe additif $(A_n[X], +)$.

★ $\forall a = (a_0, a_1, \dots, a_n) \in \ker \varphi_n$:

$$\sum_{k=0}^n \alpha_k X^k = \varphi_n(a) = 0 \Rightarrow a_0 = a_1 = \dots = a_n = 0 \Rightarrow a = (0, 0, \dots, 0).$$

Donc $\ker \varphi_n = \{(0, 0, \dots, 0)\}$. Ce qui prouve que φ_n est injectif.

★ $\forall f \in A_n[X] : \exists a_0, a_1, \dots, a_n \in A$ tq : $f = \sum_{k=0}^n a_k X^k = \varphi_n((a_0, a_1, \dots, a_n))$.

Donc φ_n est surjectif.

★ Puisque φ_n est à la fois injectif surjectif alors φ_n est bijectif.

Ce qui montre que φ_n est un isomorphisme du groupe additif $(A^{n+1}, +)$ vers le groupe additif $(A_n[X], +)$.

2) Soient n un entier naturel quelconque.

Puisque φ_n est un isomorphisme du groupe additif $(A^{n+1}, +)$ vers le groupe additif $(A_n[X], +)$ alors $(A_n[X], +)$ est isomorphe à $(A^{n+1}, +)$.

3) Soient n un entier naturel quelconque.

Puisque $(A_n[X], +)$ est isomorphe à $(A^{n+1}, +)$ alors :

$[A_n[X] \text{ est d'ordre fini}] \Leftrightarrow [A^{n+1} \text{ est d'ordre fini}] \Leftrightarrow [A \text{ est d'ordre fini}]$.

Dans ce cas : $|A_n[X]| = |A^{n+1}| = |A|^{n+1}$.

4) Soient n un entier naturel quelconque et $f = \sum_{i=0}^n a_i X^i$ un polynôme à coefficients dans A . On suppose que $n \geq 1$.

$$\begin{aligned} \text{a) } f' &= \left(\sum_{i=0}^n a_i X^i \right)' = \sum_{i=0}^n (a_i X^i)' = \sum_{i=0}^n a_i (X^i)' = a_0 (X^0)' + \sum_{i=1}^n a_i (X^i)' \\ &= a_0 (1)' + \sum_{i=1}^n a_i (i X^{i-1}) = a_0 0 + \sum_{i=1}^n i a_i X^{i-1} \\ &= \sum_{i=1}^n i a_i X^{i-1}. \end{aligned}$$

Pour tout entier naturel $i = 1, \dots, n$, posons : $i - 1 = k$, par suite on a : $i = k + 1$.

$$\begin{aligned} \text{On a donc : } f' &= \sum_{i=1}^n i a_i X^{i-1} = \sum_{k=0}^{n-1} (k+1) a_{k+1} X^k \\ &= a_1 + 2a_2 X + 3a_3 X^2 + \dots + n a_n X^{n-1} \in A[X]. \end{aligned}$$

b) Soit k un entier naturel quelconque.

$$f^{(k)} = \left(\sum_{i=0}^n a_i X^i \right)^{(k)} = \sum_{i=0}^n (a_i X^i)^{(k)} = \sum_{i=0}^n a_i (X^i)^{(k)}.$$

- Si $k \leq n$:

$$\forall i = 0, \dots, n : i < k \Rightarrow (X^i)^{(k)} = 0.$$

$$\text{Donc : } f^{(k)} = \sum_{i=k}^n a_i (X^i)^{(k)} = \sum_{i=k}^n a_i \left(\frac{i!}{(i-k)!} X^{i-k} \right) = \sum_{i=k}^n \frac{i! a_i}{(i-k)!} X^{i-k}.$$

Pour tout entier naturel $i = k, \dots, n$, posons : $i - k = j$, par suite on a : $i = j + k$.

$$\text{On a donc : } f^{(k)} = \sum_{i=k}^n \frac{i! a_i}{(i-k)!} X^{i-k} = \sum_{j=0}^{n-k} \frac{(j+k)! a_{j+k}}{j!} X^j.$$

- Si $k > n$:

$$\forall i = 0, \dots, n : (X^i)^{(k)} = 0 \text{ (car } i \leq n < k \text{)}.$$

$$\text{Donc : } f^{(k)} = \sum_{i=0}^n a_i 0 = 0.$$

Ce qui montre que :

$$\begin{cases} f^{(k)} = \sum_{i=k}^n \frac{i! a_i}{(i-k)!} X^{i-k} = \sum_{j=0}^{n-k} \frac{(j+k)! a_{j+k}}{j!} X^j & \text{si : } k \leq n \\ f^{(k)} = 0 & \text{si : } k > n \end{cases}.$$

c) Soit k un entier naturel quelconque.

- Si $k \leq n$:

$$f^{(k)} = \sum_{i=k}^n \frac{i! a_i}{(i-k)!} X^{i-k} = \sum_{j=0}^{n-k} \frac{(j+k)! a_{j+k}}{j!} X^j \in A[X].$$

- Si $k > n$:

$$f^{(k)} = 0 \in A[X].$$

d) Soient k un entier naturel tel que $k \leq n$.

Puisque $f^{(k)} = \sum_{j=0}^{n-k} \frac{(j+k)! \alpha_{j+k}}{j!} X^j$ alors le coefficient constant de $f^{(k)}$ est

$$\frac{(0+k)! \alpha_{0+k}}{0!} = \frac{k! \alpha_k}{1} = k! \alpha_k.$$

$$\begin{aligned} \text{e) } f^{(n)} &= \sum_{j=0}^{n-n} \frac{(j+n)! \alpha_{j+n}}{j!} X^j = \sum_{j=0}^0 \frac{(j+n)! \alpha_{j+n}}{j!} X^j = \frac{(0+n)! \alpha_{0+n}}{0!} X^0 = \frac{n! \alpha_n}{1} 1 \\ &= n! \alpha_n. \end{aligned}$$

Notations et définition 2-1-20 :

Soient A anneau unitaire , B un sur anneau quelconque de A (A un sous anneau de B) et $b \in B$ un élément quelconque de B .

- $\forall f = \sum_{k=0}^n \alpha_k X^k \in A[X]$: on not par $f(b)$ l'élément de B défini par :

$$f(b) = \sum_{k=0}^n \alpha_k b^k = a_0 + a_1 b + a_2 b^2 + \dots + a_n b^n$$

- $\forall f \in A[X]$: si $f(b) = 0$ on dit que b est une racine de f dans B ou b est une racine de f .

- On note par $A[b]$ l'ensemble : $A[b] = \{f(b) \mid f \in A[X]\}$.

Exemple 2-1-21 :

Soit $f = 3 - 4X + 7X^2 + 5X^3 - 2X^4 \in \mathbb{Z}[X]$.

$\mathbb{R}$ est un sur anneau de $\mathbb{Z}$ et $\sqrt{2} \in \mathbb{R}$.

$$\begin{aligned} f(\sqrt{2}) &= 3 - 4\sqrt{2} + 7(\sqrt{2})^2 + 5(\sqrt{2})^3 - 2(\sqrt{2})^4 \\ &= 3 - 4\sqrt{2} + 7 \times 2 + 5 \times 2\sqrt{2} - 2 \times 4 = 3 - 4\sqrt{2} + 14 \times 10\sqrt{2} - 8 \\ &= 9 + 6\sqrt{2}. \end{aligned}$$

Remarque 2-1-22 :

Soit A un anneau unitaire .

1) Pour tout polynôme $f = \sum_{k=0}^n \alpha_k X^k$, $f(0) = \alpha_0$ est le coefficient constant de f .

2) Pour tout polynôme f à coefficients dans A , $f(X) = f$.

3) Si B un sur anneau quelconque de A et si $b \in B$ un élément quelconque de B alors :

a) $\forall a \in A : a(b) = a$

b) $X(b) = b$

c) Pour tout entier naturel n , $X^n(b) = b^n$

4) $\forall f \in A[X]$:

a) $\forall a \in A : a(f) = a$

b) $X(f) = f$

c) $\forall n \in \mathbb{N} : X^n(f) = f^n$.

5) Si $A = \mathbb{C}$.

a) $\forall f \in \mathbb{C}[X] \text{ et } \forall a \in \mathbb{C} : \bar{f}(\bar{a}) = \overline{f(a)}$.

b) $\forall f \in \mathbb{R}[X] \text{ et } \forall a \in \mathbb{C} : f(\bar{a}) = \overline{f(a)}$.

c) Si f est un polynôme à coefficients complexes et si a est une racine complexe de f alors $\bar{a}$ est une racine complexe de $\bar{f}$.

d) Si f est un polynôme à coefficients réels et si a est une racine complexe de f alors $\bar{a}$ est aussi une racine complexe de f .

Propriétés 2-1-23 :

Soit A un anneau unitaire, B un sur anneau quelconque de A et $b \in B$ un élément quelconque de B

1) Si f et g sont des polynômes à coefficients dans A alors :

$$(f+g)(b) = f(b) + g(b).$$

2) Si a est un élément de A et si f est un polynôme à coefficients dans A alors :

$$\begin{cases} (af)(b) = a f(b) \\ (fa)(b) = f(b)a \text{ si } ab = ba \end{cases}.$$

3) Si f est un polynôme à coefficients dans A alors :

$$\forall k \in \mathbb{N} : (fX^k)(b) = f(b)b^k$$

4) Si b commute avec tous les éléments de A et si $f, g \in A[X]$ alors :

$$(fg)(b) = f(b)g(b)$$

5) Si B est abélien et si $f, g \in A[X]$ alors :

$$(fg)(b) = f(b)g(b).$$

6) Si B est abélien et si f est un polynôme à coefficients dans A alors :

$$\forall n \in \mathbb{N} : f^n(b) = f(b)^n.$$

7) Si B est abélien et si $f, g \in A[X]$ et alors :

$$f(g)(b) = f(g(b)).$$

8) Si f et g sont des polynômes à coefficients dans A et si $d^0(g) \geq 1$ alors :

$$d^0[f(g)] \leq [d^0(f)][d^0(g)].$$

9) Si B est intègre, f et g sont des polynômes à coefficients dans A et $d^0(g) \geq 1$ alors :

$$d^0[f(g)] = [d^0(f)][d^0(g)].$$

10) Si B est abélien et si f et g sont des polynômes à coefficients dans A alors :

$$[f(g)]' = f'(g)g'.$$

11) Si f est un polynôme à coefficients dans A et si a est un élément de A alors :

$$\forall k \in \mathbb{N} : [f(X+a)]^{(k)} = f^{(k)}(X+a).$$

Démonstration :

1) Soient f et g deux polynômes à coefficients dans A .

Alors il existe des éléments $\alpha_0, \alpha_1, \dots, \alpha_n, \beta_0, \beta_1, \dots, \beta_n$ de A tels que :

$$f = \sum_{k=0}^n \alpha_k X^k \quad \text{et} \quad g = \sum_{k=0}^n \beta_k X^k.$$

$$\begin{aligned}
(f+g)(b) &= \left[\sum_{k=0}^n \alpha_k X^k + \sum_{k=0}^n \beta_k X^k \right] (b) = \left[\sum_{k=0}^n (\alpha_k + \beta_k) X^k \right] (b) = \sum_{k=0}^n (\alpha_k + \beta_k) b^k \\
&= \sum_{k=0}^n (\alpha_k b^k + \beta_k b^k) = \sum_{k=0}^n \alpha_k b^k + \sum_{k=0}^n \beta_k b^k = f(b) + g(b).
\end{aligned}$$

2) Soient α un élément de A et f un polynôme à coefficients dans A .

Il existe des éléments $\beta_0, \beta_1, \dots, \beta_n$ de A tels que : $f = \sum_{k=0}^n \beta_k X^k$.

$$\begin{aligned}
\star (\alpha f)(b) &= \left(\alpha \sum_{k=0}^n \beta_k X^k \right) (b) = \left(\sum_{k=0}^n \alpha \beta_k X^k \right) (b) = \sum_{k=0}^n \alpha \beta_k b^k = \alpha \sum_{k=0}^n \beta_k b^k \\
&= \alpha f(b).
\end{aligned}$$

$\star$ Supposons que $\alpha b = b\alpha$.

$$\begin{aligned}
(f\alpha)(b) &= \left[\left(\sum_{k=0}^n \beta_k X^k \right) \alpha \right] (b) = \left(\sum_{k=0}^n \beta_k \alpha X^k \right) (b) = \sum_{k=0}^n \beta_k \alpha b^k = \sum_{k=0}^n (\beta_k b^k) \alpha \\
&= \left(\sum_{k=0}^n \beta_k b^k \right) \alpha = f(b) \alpha.
\end{aligned}$$

3) Supposons que f est un polynôme à coefficients dans A et k est un entier naturel.

Il existe des éléments $\alpha_0, \alpha_1, \dots, \alpha_n$ de A tels que : $f = \sum_{i=0}^n \alpha_i X^i$.

$$\begin{aligned}
(fX^k)(b) &= \left[\left(\sum_{i=0}^n \alpha_i X^i \right) X^k \right] (b) = \left(\sum_{i=0}^n \alpha_i X^i X^k \right) (b) = \left(\sum_{i=0}^n \alpha_i X^{i+k} \right) (b) \\
&= \left(\sum_{j=k}^{n+k} \alpha_i X^j \right) (b) = \sum_{j=k}^{n+k} \alpha_i b^j = \sum_{i=0}^n \alpha_i b^{i+k} = \sum_{i=0}^n \alpha_i b^i b^k = \left(\sum_{i=0}^n \alpha_i b^i \right) b^k \\
&= f(b) b^k \\
&\quad \forall k \in \mathbb{N} : (fX^k)(b) = f(b) b^k
\end{aligned}$$

4) Supposons que b commute avec tous les éléments de A et que $f, g \in A[X]$.

Il existe des éléments $\beta_0, \beta_1, \dots, \beta_n$ de A tels que : $g = \sum_{i=0}^n \beta_i X^i$.

$$\begin{aligned}
(fg)(b) &= \left[f \cdot \left(\sum_{i=0}^n \beta_i X^i \right) \right] (b) = \left[\sum_{i=0}^n f \cdot (\beta_i X^i) \right] (b) = \left[\sum_{i=0}^n (f\beta_i) X^i \right] (b) \\
&= \sum_{i=0}^n [(f\beta_i) X^i] (b) = \sum_{i=0}^n [(f\beta_i)(b) b^i] = \sum_{i=0}^n [f(b) \beta_i] b^i = \sum_{i=0}^n f(b) (\beta_i b^i) \\
&= f(b) \left(\sum_{i=0}^n \beta_i b^i \right) = f(b) g(b)
\end{aligned}$$

5) Supposons que B est abélien et que $f, g \in A[X]$.

Puisque B est abélien alors b commute avec tous les éléments de A .

D'après 4) on donc : $(fg)(b) = f(b)g(b)$.

6) Supposons que B est abélien et que f est un polynôme à coefficients dans A .

Montrons par récurrence que pour tout entier naturel n , $f^n(b) = f(b)^n$.

- **Pour $n = 0$:**

$$f^0(b) = f^0(b) = 1(b) = 1 = f(b)^0 = f(b)^n.$$

- **Pour $n - 1$:**

Supposons que $f^{n-1}(b) = f(b)^{n-1}$.

- **Pour n :**

Montrons qu'alors $f^n(b) = f(b)^n$.

$$f^n(b) = (f^{n-1}f)(b) = f^{n-1}(b)f(b) = f(b)^{n-1}f(b) = f(b)^n.$$

7) Supposons que B est abélien et que $f, g \in A[X]$.

Il existe des éléments $\alpha_0, \alpha_1, \dots, \alpha_n$ de A tels que : $f = \sum_{i=0}^n \alpha_i X^i$.

$$\begin{aligned} f(g)(b) &= \left[\left(\sum_{i=0}^n \alpha_i X^i \right) (g) \right] (b) = \left(\sum_{i=0}^n \alpha_i g^i \right) (b) = \sum_{i=0}^n \alpha_i \cdot (g^i(b)) = \sum_{i=0}^n \alpha_i \cdot g(b)^i \\ &= f(g(b)) \end{aligned}$$

8) Supposons que f et g sont des polynômes à coefficients dans A et que $d^0(g) \geq 1$.

- **Si $f = 0$:**

$$d^0[f(g)] = d^0[0(g)] = d^0 0 = -\infty = -\infty(d^0(g)) = [d^0(f)][d^0(g)] \leq [d^0(f)][d^0(g)].$$

- **Si $f \neq 0$:**

$$\text{Posons } d^0(f) = n. f \neq 0 \Rightarrow n = d^0(f) \in \mathbb{N}.$$

Il existe des éléments $\alpha_0, \alpha_1, \dots, \alpha_n$ de A tels que : $f = \sum_{i=0}^n \alpha_i X^i$.

$$\text{Par suite, } f(g) = \sum_{i=0}^n \alpha_i g^i.$$

$$\forall i = 0, \dots, n : d^0(\alpha_i g^i) \leq d^0(g^i) \leq i d^0 g \leq n d^0 g = [d^0(f)][d^0(g)].$$

$$\text{Donc : } d^0[f(g)] \leq \max(d^0(\alpha_0 g^0), d^0(\alpha_1 g^1), \dots, d^0(\alpha_n g^n)) \leq [d^0(f)][d^0(g)].$$

9) Supposons que B est intègre, f et g des polynômes à coefficients dans A et $d^0(g) \geq 1$.

- **Si $f = 0$:**

$$d^0[f(g)] = d^0[0(g)] = d^0 0 = -\infty = -\infty(d^0(g)) = [d^0(f)][d^0(g)].$$

- **Si $d^0 f = 0$:**

$$\text{Alors, } f \in A^*. \text{ Donc : } d^0[f(g)] = d^0(f) = 0 = 0[d^0(g)] = [d^0(f)][d^0(g)].$$

- **Si $d^0 f \geq 1$:**

$$\text{Posons } d^0(f) = n. \quad \exists \alpha_0, \alpha_1, \dots, \alpha_n \in A \text{ tq : } f = \sum_{i=0}^n \alpha_i X^i. \quad d^0(f) = n \Rightarrow \alpha_n \neq 0.$$

$$\text{Posons } f_0 = \sum_{i=0}^{n-1} \alpha_i X^i. \quad \text{Alors : } \begin{cases} f = \sum_{i=0}^n \alpha_i X^i = \sum_{i=0}^{n-1} \alpha_i X^i + \alpha_n X^n = f_0 + \alpha_n X^n \\ d^0(f_0) \leq n-1 \end{cases}.$$

$$f(g) = (f_0 + \alpha_n X^n)(g) = f_0(g) + (\alpha_n X^n)(g) = f_0(g) + \alpha_n X^n(g) = f_0(g) + \alpha_n g^n.$$

$$\alpha_n \neq 0 \Rightarrow d^0(\alpha_n g^n) = d^0(\alpha_n) + d^0(g^n) = 0 + n d^0(g) = n d^0(g).$$

$$d^0(f_0(g)) \leq [d^0(f_0)][d^0(g)] \leq (n-1)[d^0(g)] < n d^0(g) = d^0(\alpha_n g^n).$$

$$\text{Donc : } d^0[f(g)] = d^0[f_0(g) + \alpha_n g^n] = d^0(\alpha_n g^n) = n d^0(g) = [d^0(f)][d^0(g)].$$

10) Supposons que B est abélien et que f et g sont des polynômes à coefficients dans A .

Il existe des éléments $\alpha_0, \alpha_1, \dots, \alpha_n$ de A tels que : $n \geq 1$ et $f = \sum_{i=0}^n \alpha_i X^i$.

$$\begin{aligned}
[f(g)]' &= \left(\sum_{i=0}^n \alpha_i g^i \right)' = \sum_{i=0}^n (\alpha_i g^i)' = \sum_{i=0}^n \alpha_i (g^i)' = \alpha_0 (g^0)' + \sum_{i=1}^n \alpha_i (g^i)' \\
&= \alpha_0 1' + \sum_{i=1}^n \alpha_i (i g^{i-1} g') = \alpha_0 0 + \sum_{i=1}^n i \alpha_i g^{i-1} g' = 0 + \left(\sum_{i=1}^n i \alpha_i g^{i-1} \right) g' \\
&= \left(\sum_{i=1}^n i \alpha_i g^{i-1} \right) g' = \left(\sum_{i=1}^n i \alpha_i X^{i-1} \right) (g) g' = f'(g) g'
\end{aligned}$$

11) Supposons que f est un polynôme à coefficients dans A et que a est un élément de A .

Montrons par récurrence que pour tout entier naturel k , $[f(X+a)]^{(k)} = f^{(k)}(X+a)$.

- **Pour $k = 0$:**

$$[f(X+a)]^{(k)} = [f(X+a)]^{(0)} = f(X+a) = f^{(0)}(X+a) = f^{(k)}(X+a).$$

- **Pour $k - 1$:**

$$\text{Supposons que } [f(X+a)]^{(k-1)} = f^{(k-1)}(X+a).$$

- **Pour k :**

$$\text{Montrons qu'alors : } [f(X+a)]^{(k)} = f^{(k)}(X+a).$$

$$\begin{aligned}
[f(X+a)]^{(k)} &= \left[[f(X+a)]^{(k-1)} \right]' = [f^{(k-1)}(X+a)]' = [(f^{(k-1)})'(X+a)] \cdot (X+a)' \\
&= [(f^{(k)})'(X+a)] 1 = f^{(k)}(X+a).
\end{aligned}$$

Théorème 2-1-22 :

Soient A anneau unitaire, B un sur anneau quelconque de A (A un sous-anneau de B), $b \in B$ un élément quelconque de B qui commute avec tous les éléments de A (en particulier B un sur anneau abélien) et φ l'application de $A[X]$ vers B définie par : $\varphi : A[X] \rightarrow B$

$$f \mapsto \varphi(f) = f(b)$$

On a les propriétés suivantes :

- 1) φ est un homomorphisme d'anneaux.
- 2) $\forall a \in A : \varphi(a) = a$
- 3) $\varphi(X) = b$
- 4) φ est le seul homomorphisme d'anneaux Ψ de $A[X]$ vers B tel que :
 $\forall a \in A : \Psi(a) = a \quad \text{et} \quad \Psi(X) = b$
- 5) $\varphi(A[X]) = A[b]$
- 6) $A[b]$ est un sous anneau de B contenant A et b .
- 7) $A[b]$ est le plus petit sous-anneau de B contenant A et b appelé le sous-anneau de B engendré par A et b .

Démonstration :

$$1) \forall f, g \in A[X] : \begin{cases} \varphi(f+g) = (f+g)(b) = f(b) + g(b) = \varphi(f) + \varphi(g) \\ \varphi(fg) = (fg)(b) = f(b)g(b) = \varphi(f)\varphi(g) \end{cases}.$$

Donc : φ est un homomorphisme d'anneaux.

$$2) \forall a \in A : \varphi(a) = a(b) = a.$$

$$3) \varphi(X) = X(b) = b.$$

4) Soit Ψ un homomorphisme d'anneaux quelconque de $A[X]$ vers B tel que :

$$\forall a \in A : \Psi(a) = a \quad \text{et} \quad \Psi(X) = b.$$

$$\forall f \in A[X] : \exists \alpha_0, \alpha_1, \dots, \alpha_n \in A \text{ tq : } f = \sum_{i=0}^n \alpha_i X^i.$$

$$\begin{aligned} \Psi(f) &= \Psi\left(\sum_{i=0}^n \alpha_i X^i\right) = \sum_{i=0}^n \Psi(\alpha_i X^i) = \sum_{i=0}^n \Psi(\alpha_i) \Psi(X^i) = \sum_{i=0}^n \Psi(\alpha_i) \Psi(X)^i = \sum_{i=0}^n \alpha_i b^i \\ &= f(b) = \varphi(f). \end{aligned}$$

Donc $\Psi = \varphi$.

Ce qui montre que φ est le seul homomorphisme d'anneaux Ψ de $A[X]$ vers B

tel que : $\forall a \in A : \Psi(a) = a \quad \text{et} \quad \Psi(X) = b$.

5) $\varphi(A[X]) = \{\varphi(f) \text{ tq : } f \in A[X]\} = \{f(b) \text{ tq : } f \in A[X]\} = A[b]$.

6) Puisque φ est un homomorphisme d'anneaux de $A[X]$ vers B et puisque

$\varphi(A[X]) = A[b]$ alors $A[b]$ est un sous anneau de B .

$A[b]$ contient A (car on a : $\forall a \in A : a = \varphi(a) \in A[b]$).

$A[b]$ contient b (car $b = \varphi(X) \in A[b]$).

7) Soit M un sous-anneau de B contenant A et b .

$$\forall x \in A[b] : \exists f \in A[X] \text{ tq : } x = f(b).$$

$$f \in A[X] \Rightarrow \exists \alpha_0, \alpha_1, \dots, \alpha_n \in A \text{ tq : } f = \sum_{i=0}^n \alpha_i X^i.$$

$$\text{Alors : } x = f(b) = \sum_{i=0}^n \alpha_i b^i \in M.$$

Donc : $A[b] \subset M$.

Ce qui montre que $A[b]$ est le plus petit sous-anneau de B contenant A et b appelé le sous-anneau de B engendré par A et b

2-2- Formule de Mac-Laurin :

Lemme 2-2-1 :

Soient A un anneau unitaire et $f = \sum_{k=0}^n \alpha_k X^k$ un polynôme à coefficients dans A .

$$\forall k = 0, 1, 2, \dots, n : f^{(k)}(0) = k! \alpha_k.$$

En effet :

Soit k un entier naturel quelconque tel que $k \leq n$.

Puisque $k! \alpha_k$ est le coefficient constant de $f^{(k)}$ alors : $f^{(k)}(0) = k! \alpha_k$.

Remarque 2-2-2 :

Si A est un anneau unitaire intègre de caractéristique 0 alors tout entier relatif on peut confondre $n1_A$ avec n .

Lemme 2-2-3 :

Soient K corps commutatif de caractéristique 0 et $f = \sum_{k=0}^n \alpha_k X^k$ un polynôme à coefficients dans K . Pour tout entier naturel $k = 0, 1, 2, \dots, n$, $a_k = \frac{f^{(k)}(0)}{k!}$.

En effet :

Soit k un entier naturel quelconque tel que $k \leq n$.

Puisque (d'après le lemme 2-2-1) $f^{(k)}(0) = k!a_k$ alors : $a_k = \frac{f^{(k)}(0)}{k!}$.

Théorème et définition (Formule de Mac-Laurin) 2-2-4 :

Soient K corps commutatif de caractéristique 0, f un polynôme à coefficients dans K et n un entier naturel tel que $d^0(f) \leq n$. On a la formule suivante :

$$f = \sum_{k=0}^n \frac{f^{(k)}(0)}{k!} X^k = f(0) + f'(0)X + \frac{f''(0)}{2!} \dots + \frac{f^{(n)}(0)}{n!} X^n.$$

appelée la formule de Mac-Laurin appliquée au polynôme f .

Démonstration :

$$d^0(f) \leq n \Rightarrow \exists \alpha_0, \alpha_1, \dots, \alpha_n \in A \text{ tq : } f = \sum_{i=0}^n \alpha_i X^i.$$

D'après le lemme 2-2-3, $a_k = \frac{f^{(k)}(0)}{k!}$ pour tout entier naturel $k = 0, 1, 2, \dots, n$.

Ce qui montre que : $f = \sum_{k=0}^n \frac{f^{(k)}(0)}{k!} X^k = f(0) + f'(0)X + \frac{f''(0)}{2!} \dots + \frac{f^{(n)}(0)}{n!} X^n$.

appelée la formule de Mac-Laurin appliquée au polynôme f .

2-3- Formule de Taylor :**Théorème et définition (Formule de Taylor) 2-3-1 :**

Soient K corps commutatif de caractéristique 0, f un polynôme à coefficients dans K , α un élément de K et n un entier naturel tel que $d^0(f) \leq n$. On a la formule suivante :

$$f = \sum_{k=0}^n \frac{f^{(k)}(\alpha)}{k!} (X - \alpha)^k = f(\alpha) + f'(\alpha)(X - \alpha) + \frac{f''(\alpha)}{2!} (X - \alpha)^2 + \dots + \frac{f^{(n)}(\alpha)}{n!} (X - \alpha)^n.$$

appelée la formule de Taylor appliquée au polynôme f et α .

Démonstration :

Posons $g = f(X + a)$. On a : $d^0(g) = d^0[f(X + a)] = [d^0(f)][d^0(X + a)] = d^0(f) \leq n$

Pour tout entier naturel $k = 0, 1, 2, \dots, n$:

$$g^{(k)} = [f(X + a)]^{(k)} = f^{(k)}(X + a) \text{ par suite on a :}$$

$$g^{(k)}(0) = [f^{(k)}(X + a)](0) = f^{(k)}(X + a)(0) = f^{(k)}(a).$$

D'après la formule de Mac-Laurin appliquée au polynôme g on a donc :

$$g = \sum_{k=0}^n \frac{g^{(k)}(0)}{k!} X^k = \sum_{k=0}^n \frac{f^{(k)}(a)}{k!} X^k$$

$$\text{Ce qui montre que : } f = f(X) = f(X - a + a) = g(X - a) = \sum_{k=0}^n \frac{f^{(k)}(a)}{k!} (X - a)^k.$$

Exemple 2-3-2 :

Soient $f = 3 - 4X + 7X^2 + 5X^3 - 2X^4 \in \mathbb{Q}[X]$ et $\alpha = 2$.

La formule de Taylor appliquée au polynôme f et 2 est :

$$f = f(2) + f'(2)(X - 2) + \frac{f''(2)}{2!}(X - 2)^2 + \frac{f'''(2)}{3!}(X - 2)^3 + \frac{f^{(4)}(2)}{4!}(X - 2)^4.$$

$$f(2) = 3 - 8 + 28 + 40 - 32 = 31.$$

$$f' = -4 + 14X + 15X^2 - 8X^3 \Rightarrow f'(2) = -4 + 28 + 60 - 64 = 20.$$

$$f'' = 14 + 30X - 24X^2 \Rightarrow \frac{f''(2)}{2!} = \frac{14 + 60 - 96}{2} = \frac{-22}{2} = -11.$$

$$f''' = 30 - 48X \Rightarrow \frac{f'''(2)}{3!} = \frac{30 - 96}{6} = -11.$$

$$f^{(4)} = -48 \Rightarrow \frac{f^{(4)}(2)}{4!} = \frac{-48}{24} = -2.$$

$$\text{Donc : } f = 31 + 20(X - 2) - 11(X - 2)^2 - 11(X - 2)^3 - 2(X - 2)^4.$$

3- Division, divisibilité et fonctions polynômiales :

Dans tout le paragraphe, K étant un anneau commutatif unitaire non nul.

3-1-Division euclidienne :

Lemme 3-1-1 :

Soient A, B, Q et R des polynômes à coefficients dans K tels que :
$$\begin{cases} A = BQ + R \\ d^0 R < d^0 B \end{cases}.$$

Si le coefficient dominant de B est inversible et si $d^0 A < d^0 B$ alors : $Q = 0$ et $R = A$.

Démonstration :

$$A = BQ + R \Rightarrow BQ = A - R \Rightarrow d^0(BQ) = d^0(A - R) \leq \max(d^0 A, d^0 R) < d^0 B.$$

Puisque le coefficient dominant de B est inversible alors :

$$d^0 B + d^0 Q = d^0(BQ) < d^0 B \Rightarrow d^0 Q < 0 \Rightarrow d^0 Q = -\infty \Rightarrow Q = 0.$$

$$R = 0 + R = B \cdot 0 + R = BQ + R = A.$$

Donc : $Q = 0$ et $R = A$.

Lemme 3-1-2 :

Soient A, B, Q, R, U et V des polynômes à coefficients dans K tels que :

$$\begin{cases} A = BU + V = BQ + R \\ d^0 V < d^0 B \text{ et } d^0 R < d^0 B \end{cases}.$$

Si le coefficient dominant de B est inversible alors $U = Q$ et $V = R$.

Démonstration :

$$A = BU + V = BQ + R \Rightarrow 0 = (BU + V) - (BQ + R) = BU + V - BQ - R \\ = B \cdot (U - Q) + V - R.$$

$$d^0(V - R) \leq \max(d^0 V, d^0 R) < d^0 B.$$

Puisque le coefficient dominant de B est inversible, $d^0 0 = -\infty < d^0 B$,

$0 = B \cdot (U - Q) + V - R$ et $d^0(V - R) < d^0 B$ alors (d'après le lemme 3-1-1) :

$$\begin{cases} U - Q = 0 \\ V - R = 0 \end{cases} \Rightarrow \begin{cases} U = Q \\ V = R \end{cases}.$$

Lemme 3-1-3 :

Soit B un polynôme non nul à coefficients dans K de degré $m \geq 1$.

Si le coefficient dominant de B est inversible alors pour tout entier naturel n et pour tout polynôme $A \in K_n[X]$ il existe d'une façon unique, deux polynômes Q et R à coefficients

dans K tels que :
$$\begin{cases} A = BQ + R \\ d^0 R < d^0 B \end{cases}.$$

Démonstration :

$$d^0 B = m \Rightarrow \exists b_0, b_1, \dots, b_m \in K \text{ tq : } \left[B = \sum_{i=0}^m b_i X^i \text{ et } b_m \neq 0 \right].$$

Supposons que le coefficient dominant b_m de B est inversible.

Montrons par récurrence que pour tout entier naturel n et pour tout polynôme

$A \in K_n[X]$ il existe d'une façon unique, deux polynômes Q et R à coefficients dans K

tels que :
$$\begin{cases} A = BQ + R \\ d^0 R < d^0 B \end{cases}.$$

- **Pour $n = 0$:**

Soit A un élément quelconque de $K_n[X] = K_0[X] = K$.

• **Existence :**

Il suffit de prendre $Q = 0$ et $R = A$ et on a :
$$\begin{cases} A = 0 + A = B \cdot 0 + A = BQ + R \\ d^0 R = d^0 A \leq 0 < 1 \leq d^0 B \end{cases}.$$

D'où l'existence.

• **Unicité :**

Soient U et V deux polynômes à coefficients dans K tels que :
$$\begin{cases} A = BU + V \\ d^0 V < d^0 B \end{cases}.$$

D'après le lemme 3-1-2, puisqu'on a :
$$\begin{cases} A = BU + V = BQ + R \\ d^0 V < d^0 B \text{ et } d^0 R < d^0 B \end{cases}.$$

et puisque le coefficient dominant de B est inversible alors $U = Q$ et $V = R$.

D'où l'unicité.

- **Pour $n - 1$:**

Supposons que pour tout polynôme $A \in K_{n-1}[X]$ il existe d'une façon unique, deux

polynômes Q et R à coefficients dans K tels que :
$$\begin{cases} A = BQ + R \\ d^0 R < d^0 B \end{cases}.$$

- **Pour n :**

Montrons que pour tout polynôme $A \in K_n[X]$ il existe d'une façon unique, deux

polynômes Q et R à coefficients dans K tels que :
$$\begin{cases} A = BQ + R \\ d^0 R < d^0 B \end{cases}.$$

Soit A un élément quelconque de $K_n[X]$.

• **Existence :**

★ **Si $n < m = d^0 B$:**

Il suffit de prendre, $Q = 0$ et $R = A$. On alors :
$$\begin{cases} A = 0 + A = B0 + A = BQ + R \\ d^0 R = d^0 A \leq n < d^0 B \end{cases}.$$

D'où l'existence.

★ **Si $n \geq m = d^0 B$:**

Soient $a_0, a_1, \dots, a_n$ les éléments de K tels que $A = \sum_{k=0}^n a_k X^k$.

Posons $M = a_n b_m^{-1} X^{n-m} B$.
$$M = a_n b_m^{-1} X^{n-m} \left(\sum_{i=0}^m b_i X^i \right) = \sum_{i=0}^m a_n b_m^{-1} b_i X^{i+n-m}$$

Pour tout entier naturel $i = 0, \dots, m$, posons : $k = i + n - m$ alors : $i = k + m - n$.

Donc :
$$M = \sum_{k=n-m}^n a_n b_m^{-1} b_{k+m-n} X^k$$

Pour tout entier naturel $k = 0, \dots, n$, posons :
$$\begin{cases} d_k = a_n b_m^{-1} b_{k+m-n} & \text{si } k \geq n - m \\ d_k = 0 & \text{si } k < n - m \end{cases}.$$

Alors : $M = \sum_{k=0}^n d_k X^k$. Posons : $A_0 = A - M$.

$$A_0 = A - M = \sum_{k=0}^n a_k X^k - \sum_{k=0}^n d_k X^k = \sum_{k=0}^n (a_k - d_k) X^k.$$

$$a_n - d_n = a_n - a_n b_m^{-1} b_{n+m-n} = a_n - a_n b_m^{-1} b_m = a_n - a_n 1 = a_n - a_n = 0.$$

Donc : $A_0 = \sum_{k=0}^{n-1} (a_k - d_k) X^k \in K_{n-1}[X]$.

D'après l'hypothèse de récurrence, il existe d'une façon unique, deux polynômes

Q_0 et R à coefficients dans K tels que :
$$\begin{cases} A_0 = BQ_0 + R \\ d^0 R < d^0 B \end{cases}.$$

Par suite on a :

$$\begin{aligned} A &= A - M + M = A_0 + M = BQ_0 + R + a_n b_m^{-1} X^{n-m} B = BQ_0 + a_n b_m^{-1} X^{n-m} B + R \\ &= B(Q_0 + a_n b_m^{-1} X^{n-m}) + R. \end{aligned}$$

$$\text{Pour } Q = Q_0 + a_n b_m^{-1} X^{n-m} \text{ on a : } \begin{cases} A = BQ + R \\ d^0 R < d^0 B \end{cases}.$$

D'où l'existence.

• **Unicité :**

$$\text{Soient } U \text{ et } V \text{ deux polynômes à coefficients dans } K \text{ tels que : } \begin{cases} A = BU + V \\ d^0 V < d^0 B \end{cases}.$$

$$\text{D'après le lemme 3-1-2, puisqu'on a : } \begin{cases} A = BU + V = BQ + R \\ d^0 V < d^0 B \text{ et } d^0 R < d^0 B \end{cases}.$$

et puisque le coefficient dominant de B est inversible alors $U = Q$ et $V = R$.
D'où l'unicité.

Théorème et définition 3-1-4 :

Soient A et B deux polynômes à coefficients dans K .

Si $B \neq 0$ et si le coefficient dominant de B est inversible alors il existe d'une façon unique, deux polynômes $Q, R \in K[X]$ à coefficients dans K tels que :

$$\begin{cases} A = BQ + R \\ d^0 R < d^0 B \end{cases}.$$

Le polynôme Q est appelé le quotient de la division euclidienne de A par B ou le quotient de A par B .

Le polynôme R est appelé le reste de la division euclidienne de A par B ou le reste de A par B .

La recherche des polynômes Q et R est appelé la division euclidienne de A par B ou la division de A par B .

Démonstration :

★ **Si $d^0 B = 0$:**

• **Existence :**

$d^0 B = 0 \Rightarrow B \in K^*$. Par suite le coefficient dominant B de B est inversible.

$$\text{Il suffit de prendre } Q = B^{-1}A \text{ et } R = 0 \text{ et on a : } \begin{cases} A = B(B^{-1}A) + 0 = BQ + A \\ d^0 R = d^0 0 = -\infty < d^0 B \end{cases}.$$

D'où l'existence.

• **Unicité :**

$$\text{Soient } U \text{ et } V \text{ deux polynômes à coefficients dans } K \text{ tels que : } \begin{cases} A = BU + V \\ d^0 V < d^0 B \end{cases}.$$

$$\text{D'après le lemme 3-1-2, puisqu'on a : } \begin{cases} A = BU + V = BQ + R \\ d^0 V < d^0 B \text{ et } d^0 R < d^0 B \end{cases}.$$

et puisque le coefficient dominant de B est inversible alors $U = Q$ et $V = R$.
D'où l'unicité.

★ Si $d^0 B \geq 1$:

Il existe des éléments $a_0, a_1, \dots, a_n$ de A tels que : $A = \sum_{k=0}^n a_k X^k$, alors $A \in K_n[X]$.

D'après le lemme 3-1-3, puisque $d^0 B \geq 1$, le coefficient dominant de B est inversible, n est un entier naturel et $A \in K_n[X]$, alors il existe d'une façon unique, deux

polynômes Q et R à coefficients dans K tels que :
$$\begin{cases} A = BQ + R \\ d^0 R < d^0 B \end{cases}.$$

Corollaire 3-1-5 :

Soient A et B deux polynômes à coefficients dans K .

Si B est unitaire alors le quotient et le reste de la division euclidienne de A par B existent.

En effet :

Supposons que B est unitaire.

Alors le coefficient dominant de B est inversible.

D'après le théorème et définition 3-1-4, le quotient et le reste de la division euclidienne de A par B existent alors.

Corollaire 3-1-6 :

Soient A et B deux polynômes à coefficients dans K .

Si B est non nul et si K est un corps commutatif alors le quotient et le reste de la division euclidienne de A par B existent.

En effet :

Supposons que B est non nul et que K est un corps commutatif.

Alors le coefficient dominant de B est inversible.

D'après le théorème et définition 3-1-4, le quotient et le reste de la division euclidienne de A par B existent alors.

Exemple 3-1-7 :

Si $K = \mathbb{Q}$.

Soient $A = 6X^5 + 5X^4 - 4X^3 - 5X^2 - 2$ et $B = 2X^3 + 3X^2 - 5$.

$$\begin{array}{r|l} A = 6X^5 + 5X^4 - 4X^3 - 5X^2 - 2 & B = 2X^3 + 3X^2 - 5 \\ -6X^5 - 9X^4 & + 15X^2 \\ \hline -4X^4 - 4X^3 + 10X^2 - 2 & \\ 4X^4 + 6X^3 & - 10X \\ \hline 2X^3 + 10X^2 - 10X - 2 & \\ -2X^3 - 3X^2 & + 5 \\ \hline R = 7X^2 - 10X + 3 & \end{array}.$$

Donc : $Q = 3X^2 - 2X + 1$ est le quotient de la division euclidienne de A par B .

et $R = 7X^2 - 10X + 3$ est le reste de la division euclidienne de A par B .

Propriétés 3-1-8 :

Soient A et B deux polynômes à coefficients dans K .

On suppose que $B \neq 0$ et que le coefficient dominant de B est inversible.

Soient Q le quotient de la division euclidienne de A par B et R le reste de la division euclidienne de A par B .

1) Si $K = \mathbb{C}$ alors $\overline{Q}$ est le quotient de la division euclidienne de $\overline{A}$ par $\overline{B}$ et $\overline{R}$ est le reste de la division euclidienne de $\overline{A}$ par $\overline{B}$.

2) Si B est une constante inversible $\alpha \in U(K)$ alors :
$$\begin{cases} Q = \alpha^{-1}A \\ R = 0 \end{cases}$$

3) Si K est un corps commutatif et si B est une constante non nulle α alors :

$$\begin{cases} Q = \alpha^{-1}A \\ R = 0 \end{cases}.$$

4) $d^0A < d^0B$ alors :
$$\begin{cases} Q = 0 \\ R = A \end{cases}.$$

5) Si $\alpha \in K$ et si $B = X - \alpha$ alors. $R = A(\alpha)$.

En effet :

Supposons que $\alpha \in K$ et que $B = X - \alpha$.

$$d^0R < d^0B = d^0(X - \alpha) = 1 \Rightarrow d^0R \leq 0 \Rightarrow R \in K.$$

$$\begin{aligned} A = BQ + R &= (X - \alpha)Q + R \Rightarrow A(\alpha) = [(X - \alpha)Q + R](\alpha) = (\alpha - \alpha)Q(\alpha) + R(\alpha) \\ &\Rightarrow A(\alpha) = 0Q(\alpha) + R = 0 + R = R. \end{aligned}$$

Donc : $R = A(\alpha)$.

Exemple :

Si $K = \mathbb{R}$.

Soient $A = 2X^5 - 7X^4 + 5X^2 + 13X + 6$ et $\alpha = 3$

$$\begin{aligned} R = A(3) &= 2 \times 3^5 - 7 \times 3^4 + 5 \times 3^2 + 13 \times 3 + 6 \\ &= 2 \times 243 - 7 \times 81 + 5 \times 9 + 39 + 6 \\ &= 486 - 567 + 45 + 45 = 9 \end{aligned}$$

Donc le reste de la division euclidienne de A par $X - 3$ est $R = A(3) = 9$.

3-2-Développement suivant les puissances d'un polynôme :

Définition 3-2-1 :

Soient $A, A_0, \dots, A_n, P$ des polynômes à coefficients dans K . Si on a les deux propriétés suivantes :

i) $A = \sum_{k=0}^n A_k P^k = A_0 + A_1 P + \dots + A_n P^n.$

ii) $\forall k = 0, \dots, n : d^0 A_k < d^0 P.$

On dit que $A = \sum_{k=0}^n A_k P^k$ est un développement de A suivant les puissances de P .

Proposition 3-2-2 :

Soient A un polynôme à coefficients dans K et α un élément de K .

Un développement de A suivant les puissances de $X - \alpha$ est de la forme :

$$A = \sum_{k=0}^n a_k (X - \alpha)^k = a_0 + a_1(X - \alpha) + \dots + a_n(X - \alpha)^n, \text{ où } a_0, a_1, \dots, a_n \text{ sont}$$

des éléments de K .

Démonstration :

Soit $A = \sum_{k=0}^n A_k (X - \alpha)^k$ un développement de A suivant les puissances de $X - \alpha$.

On a : $\forall k = 0, \dots, n : d^0 A_k < d^0 (X - \alpha) = 1 \Rightarrow d^0 A_k \leq 0 \Rightarrow \exists a_k \in K \text{ tq : } A_k = a_k$.

Donc $a_0, a_1, \dots, a_n$ sont des éléments de K et $A = \sum_{k=0}^n a_k (X - \alpha)^k$ est un

développement de A suivant les puissances de $X - \alpha$.

Proposition 3-2-3 :

Soient A et P deux polynômes à coefficients dans K .

i) Si A admet un développement suivant les puissances de P alors P est non nul.

ii) Si $A = \sum_{k=0}^n A_k P^k$ est un développement de A suivant les puissances de P alors

$$d^0 A < (n + 1) d^0 P.$$

En particulier :

Si $\alpha \in K$ et si $A = \sum_{k=0}^n a_k (X - \alpha)^k$ est un développement de A suivant les puissances

de $X - \alpha$ alors $d^0 A \leq n$.

Démonstration :

i) Si A admet un développement suivant les puissances de P alors il existe des polynômes $A_0, \dots, A_n \in K[X]$ tels que :

$$\begin{cases} A = \sum_{k=0}^n A_k P^k \\ \forall k = 0, \dots, n : d^0 A_k < d^0 P \end{cases}$$

alors : $d^0 A_0 < d^0 P \Rightarrow d^0 P \neq -\infty \Rightarrow P \neq 0$.

ii) Supposons que $A = \sum_{k=0}^n A_k P^k$ est un développement de A suivant les puissances

de P .

$$\forall k = 0, \dots, n : d^0 (A_k P^k) \leq d^0 A_k + d^0 P^k \leq d^0 A_k + k d^0 P \leq d^0 A_k + n d^0 P < d^0 P + n d^0 P$$

On a alors : $\forall k = 0, \dots, n : d^0 (A_k P^k) < (n + 1) d^0 P$

Ce qui montre que : $d^0 A = d^0 \left(\sum_{k=0}^n A_k P^k \right) < (n + 1) d^0 P$.

En particulier :

Si $\alpha \in K$ et si $A = \sum_{k=0}^n a_k (X - \alpha)^k$ est un développement de A suivant les puissances de $X - \alpha$ alors : $d^0 A < (n+1)d^0(X - \alpha) = n+1 \Rightarrow d^0 A \leq n$.

Théorème 3-2-4 :

Soient A un polynôme à coefficients dans K et P un polynôme non constant à coefficients dans K (c'est à dire $d^0 P \geq 1$) de coefficient dominant inversible.

Pour tout entier naturel n tel que $d^0 A < (n+1)d^0 P$, le polynôme A admet un

et un seul développement suivant les puissances de P de la forme $A = \sum_{k=0}^n A_k P^k$.

Démonstration :

Par récurrence sur $n \in \mathbb{N}$.

- **Pour $n = 0$:**

On a : $d^0 A < d^0 P$.

• **Existence :**

Il suffit de prendre $A_0 = A$ et on a alors : $A = A_0 = \sum_{k=0}^0 A_k P^k$ et $d^0 A_0 < d^0 P$.

Donc : $A = \sum_{k=0}^0 A_k P^k$ est un développement de A suivant les puissances de P .

• **Unicité :**

Soit $B_0 \in K[X]$ tel que : $A = \sum_{k=0}^0 B_k P^k$ et $d^0 B_0 < d^0 P$.

Alors : $B_0 = \sum_{k=0}^0 B_k P^k = A = \sum_{k=0}^0 A_k P^k = A_0$.

D'où l'unicité du développement de A suivant les puissances de P .

- **Pour $n = 1$:**

Supposons que si $d^0 A < nd^0 P$, le polynôme A admet un et un seul développement

suivant les puissances de P de la forme $A = \sum_{k=0}^{n-1} A_k P^k$.

- **Pour n :**

Montrons qu'alors si $d^0 A < (n+1)d^0 P$, le polynôme A admet un et un seul

développement suivant les puissances de P de la forme $A = \sum_{k=0}^n A_k P^k$.

On suppose que $d^0 A < (n+1)d^0 P$.

• **Existence :**

Soient Q le quotient de la division euclidienne de A par P et A_0 le reste de la division euclidienne de A par P .

On a alors : $A = QP + A_0$ et $d^0 A_0 < d^0 P$.

$$d^0 A_0 < d^0 P \Rightarrow d^0 A_0 < (n+1)d^0 P \Rightarrow d^0(A - A_0) \leq \max(d^0 A, d^0 A_0) < (n+1)d^0 P.$$

$$A = QP + A_0 \Rightarrow QP = A - A_0 \Rightarrow d^0(QP) = d^0(A - A_0) < (n+1)d^0 P.$$

Puisque le coefficient dominant de P est inversible alors :

$$d^0 Q + d^0 P = d^0(QP) < (n+1)d^0 P = nd^0 P + d^0 P \Rightarrow d^0 Q < nd^0 P.$$

D'après l'hypothèse de récurrence, Q admet un et un seul développement

$$\text{suivant les puissances de } P \text{ de la forme } Q = \sum_{k=0}^{n-1} Q_k P^k.$$

$$\text{Alors : } A = A_0 + QP = A_0 + \left(\sum_{i=0}^{n-1} Q_i P^i \right) P = A_0 + \sum_{i=0}^{n-1} Q_i P^{i+1} = A_0 + \sum_{k=1}^n Q_{k-1} P^k.$$

Pour tout entier $k = 1, \dots, n$, posons $A_k = Q_{k-1}$. On a alors :

$$\begin{cases} A = \sum_{k=0}^n A_k P^k \\ \forall k = 0, \dots, n : d^0 A_k < d^0 P \end{cases}.$$

Donc $A = \sum_{k=0}^n A_k P^k$ est un développement de A suivant les puissances de P

Doù l'existence.

• **Unicité :**

Soit $A = \sum_{k=0}^n M_k P^k$ un développement quelconque de A suivant les puissances de P .

$$A = \sum_{i=0}^n M_i P^i \Rightarrow A = M_0 + \sum_{i=1}^n M_i P^i = M_0 + \left(\sum_{i=1}^n M_i P^{i-1} \right) P \text{ et } d^0 M_0 < d^0 P.$$

$$\text{On a alors : } A = M_0 + \left(\sum_{k=0}^{n-1} M_{k+1} P^k \right) P \text{ et } d^0 M_0 < d^0 P.$$

Donc $\sum_{k=0}^{n-1} M_{k+1} P^k$ est le quotient de la division euclidienne de A par P et M_0 est le reste de la division euclidienne de A par P .

$$\text{Par suite : } \sum_{k=0}^{n-1} M_{k+1} P^k = Q \text{ et } M_0 = A_0.$$

Pour tout entier $k = 0, \dots, n-1$, posons $N_k = M_{k+1}$. On a alors :

$$\begin{cases} Q = \sum_{k=0}^{n-1} M_{k+1} P^k = \sum_{k=0}^{n-1} N_k P^k \\ \forall k = 0, \dots, n-1 : d^0 N_k = d^0 M_{k+1} < d^0 P \end{cases}.$$

D'après l'hypothèse de récurrence on a : $\forall k = 0, \dots, n-1 : N_k = Q_k$.

$$\text{Alors : } \forall k = 1, \dots, n : M_k = N_{k-1} = Q_{k-1} = A_k.$$

$$\text{Ce qui montre que : } \forall k = 0, \dots, n : M_k = N_{k-1} = Q_{k-1} = A_k.$$

D'où l'unicité du développement de A suivant les puissances de P .

Corollaire 3-2-5 :

Soient A un polynôme à coefficients dans K et α un élément de K .

Pour tout entier naturel $n \geq d^0 A$, le polynôme A admet un et un seul

développement suivant les puissances de $X - \alpha$ de la forme $A = \sum_{k=0}^n a_k (X - \alpha)^k$.

Démonstration :

Soit n un entier naturel tel que $n \geq d^0 A$.

$d^0 A \leq n \Rightarrow d^0 A < n + 1 = (n + 1)d^0 (X - \alpha)$.

Ce qui montre (d'après le théorème précédent) que le polynôme A admet un et un

seul développement suivant les puissances de $X - \alpha$ de la forme $A = \sum_{k=0}^n a_k (X - \alpha)^k$.

Corollaire 3-2-6 :

Pour tout polynôme A à coefficients dans K et pour tout polynôme non constant P à coefficients dans K (c'est à dire $d^0 P \geq 1$) de coefficient dominant inversible, le polynôme A admet un développement suivant les puissances de P .

Démonstration :

Soient A un polynôme à coefficients dans K et P un polynôme non constant à coefficients dans K de coefficient dominant inversible.

Puisque $d^0 P \geq 1$ alors il existe alors entier naturel n tel que $d^0 A < (n + 1)d^0 P$

Donc (d'après le théorème précédent), A admet un développement suivant les puissances de P .

Exmple 3-2-7 :

Dans $\mathbb{Z}$, soient $A = X^7 - 5X^6 + 15X^5 - 26X^4 + 33X^3 - 20X^2 + 6X + 7$ et $P = X^2 - 2X + 3$.

$$\begin{array}{r}
 A = X^7 - 5X^6 + 15X^5 - 26X^4 + 33X^3 - 20X^2 + 6X + 7 \\
 \underline{-X^7 + 2X^6 - 3X^5} \\
 -3X^6 + 12X^5 - 26X^4 + 33X^3 - 20X^2 + 6X + 7 \\
 \underline{3X^6 - 6X^5 + 9X^4} \\
 6X^5 - 17X^4 + 33X^3 - 20X^2 + 6X + 7 \\
 \underline{-6X^5 + 12X^4 - 18X^3} \\
 -5X^4 + 15X^3 - 20X^2 + 6X + 7 \\
 \underline{5X^4 - 10X^3 + 15X^2} \\
 5X^3 - 5X^2 + 6X + 7 \\
 \underline{-5X^3 + 10X^2 - 15X} \\
 5X^2 - 9X + 7 \\
 \underline{-5X^2 + 10X - 15} \\
 X - 8
 \end{array}$$

$$\begin{array}{r}
 P = X^2 - 2X + 3 \\
 \hline
 X^5 - 3X^4 + 6X^3 - 5X^2 + 5X + 5
 \end{array}$$

$$\begin{array}{r|l}
 X^5 - 3X^4 + 6X^3 - 5X^2 + 5X + 5 & P = X^2 - 2X + 3 \\
 -X^5 + 2X^4 - 3X^3 & \hline
 -X^4 + 3X^3 - 5X^2 + 5X + 5 & \\
 X^4 - 2X^3 + 3X^2 & \\
 \hline
 X^3 - 2X^2 + 5X + 5 & \\
 -X^3 + 2X^2 - 3X & \\
 \hline
 2X + 5 &
 \end{array}$$

$$\begin{array}{r|l}
 X^3 - X^2 + X & P = X^2 - 2X + 3 \\
 -X^3 + 2X^2 - 3X & \\
 \hline
 3X^2 - 2X & \\
 -3X^2 + 6X - 9 & \\
 \hline
 4X - 9 &
 \end{array}$$

Donc : $A = X - 8 + (2X + 5)P + (4X - 9)P^2 + (X + 3)P^3$
 $= X - 8 + (2X + 5)(X^2 - 2X + 3) + (4X - 9)(X^2 - 2X + 3)^2 + (X + 3)(X^2 - 2X + 3)^3$
est le développement du polynôme $A = X^7 - 5X^6 + 15X^5 - 26X^4 + 33X^3 - 20X^2 + 6X + 7$
suivant les puissances de $P = X^2 - 2X + 3$.

Corollaire 3-2-8 :

Soient P un polynôme non constant à coefficients dans K (c'est à dire $d^0P \geq 1$) de coefficient dominant inversible et $A_0, \dots, A_n, B_0, \dots, B_n$ des polynômes à coefficients dans K tels que : $\forall k = 0, \dots, n : [d^0A_k < d^0P \text{ et } d^0B_k < d^0P]$.

Si $\sum_{k=0}^n A_k P^k = \sum_{k=0}^n B_k P^k$ alors : $\forall k = 0, \dots, n : A_k = B_k$.

Démonstration :

Supposons que $\sum_{k=0}^n A_k P^k = \sum_{k=0}^n B_k P^k$ et posons $A = \sum_{k=0}^n A_k P^k = \sum_{k=0}^n B_k P^k$.

Comme on a : $\forall k = 0, \dots, n : [d^0A_k < d^0P \text{ et } d^0B_k < d^0P]$. alors :

$A = \sum_{k=0}^n A_k P^k$ et $A = \sum_{k=0}^n B_k P^k$ sont des développements de A suivant les puissances

de P . Donc (d'après la proposition 3-2-3) on a : $d^0A < (n+1)d^0P$.

Ce qui montre (d'après le théorème 3-2-4) que : $\forall k = 0, \dots, n : A_k = B_k$.

Corollaire 3-2-9 :

Soient $\alpha, a_0, \dots, a_n, b_0, \dots, b_n$ des éléments de K .

Si $\sum_{k=0}^n a_k (X - \alpha)^k = \sum_{k=0}^n b_k (X - \alpha)^k$ alors : $\forall k = 0, \dots, n : a_k = b_k$.

Démonstration :

Supposons que $\sum_{k=0}^n a_k(X - \alpha)^k = \sum_{k=0}^n b_k(X - \alpha)^k$ et posons :

$$A = \sum_{k=0}^n a_k(X - \alpha)^k = \sum_{k=0}^n b_k(X - \alpha)^k.$$

On a : $\forall k = 0, \dots, n : [d^0 a_k \leq 0 < 1 = d^0(X - \alpha) \text{ et } d^0 b_k \leq 0 < 1 = d^0(X - \alpha)]$.

Donc (d'après le corollaire 3-2-8) on a : $\forall k = 0, \dots, n : a_k = b_k$.

Corollaire 3-2-10 :

Soient P un polynôme non constant à coefficients dans K (c'est à dire $d^0 P \geq 1$) de coefficient dominant inversible et $A_0, \dots, A_n$ des polynômes à coefficients dans K tels que : $\forall k = 0, \dots, n : d^0 A_k < d^0 P$.

Si $\sum_{k=0}^n A_k P^k = 0$ alors : $A_0 = \dots = A_n = 0$.

Démonstration :

Supposons que $\sum_{k=0}^n A_k P^k = 0$. Alors on a : $\sum_{k=0}^n A_k P^k = \sum_{k=0}^n 0 P^k$.

Donc (d'après le corollaire 3-2-9) on a : $\forall k = 0, \dots, n : A_k = 0$.

Par suite on a : $A_0 = \dots = A_n = 0$.

Corollaire 3-2-11 :

Soient $\alpha, a_0, \dots, a_n$ des éléments de K .

Si $\sum_{k=0}^n a_k(X - \alpha)^k = 0$ alors : $a_0 = \dots = a_n = 0$.

Démonstration :

Supposons que $\sum_{k=0}^n a_k(X - \alpha)^k = 0$.

On a : $\forall k = 0, \dots, n : d^0 a_k \leq 0 < 1 = d^0(X - \alpha)$.

Donc (d'après le corollaire 3-2-10) on a : $a_0 = \dots = a_n = 0$.

Corollaire 3-2-12 :

Soient A un polynôme à coefficients dans K et α un élément de K .

Si K est un corps commutatif de caractéristique 0 alors le développement de A suivant les puissances de $X - \alpha$ est égale à la formule de Taylor appliquée au polynôme A et α , c'est à dire, si n est un entier naturel et si $d^0 A \leq n$ alors :

$$\begin{aligned} A &= \sum_{k=0}^n \frac{A^{(k)}(\alpha)}{k!} (X - \alpha)^k \\ &= A(\alpha) + A'(\alpha)(X - \alpha) + \frac{A''(\alpha)}{2!} (X - \alpha)^2 + \dots + \frac{A^{(n)}(\alpha)}{n!} (X - \alpha)^n \end{aligned}$$

est le développement de A suivant les puissances de $X - \alpha$.

3-3-Procédé de Hôrner :

Soient $A = \sum_{k=0}^n a_k X^k = a_0 + a_1 X + \dots + a_n X^n \in K[X]$ où $n \geq 2$, $\alpha \in K$,

M le quotient de la division euclidienne A par $X - \alpha$ et R le reste de la division euclidienne A par $X - \alpha$.

Alors : $\begin{cases} A = (X - \alpha)Q + R \\ d^0 R < d^0(X - \alpha) = 1 \end{cases}$. Donc : $d^0 R \leq 0 \Rightarrow R \in K$.

$$\begin{aligned} A = (X - \alpha)Q + R &\Rightarrow (X - \alpha)Q = A - R \Rightarrow d^0[(X - \alpha)Q] = d^0(A - R) \leq \max(d^0 A, d^0 R) \\ &\Rightarrow d^0(X - \alpha) + d^0 Q \leq \max(d^0 A, 0) \leq n \Rightarrow 1 + d^0 Q \leq n \\ &\Rightarrow d^0 Q \leq n - 1 \end{aligned}$$

$$\Rightarrow \exists b_0, b_1, \dots, b_{n-1} \in K \text{ tq : } Q = \sum_{k=0}^{n-1} b_k X^k.$$

Par suite on a : $\sum_{k=0}^n a_k X^k = A = (X - \alpha)Q + R = (X - \alpha) \left(\sum_{i=0}^{n-1} b_i X^i \right) + R$

$$\begin{aligned} &= X \left(\sum_{i=0}^{n-1} b_i X^i \right) - \alpha \left(\sum_{i=0}^{n-1} b_i X^i \right) + R \\ &= \sum_{i=0}^{n-1} b_i X^{i+1} - \sum_{i=0}^{n-1} \alpha b_i X^i + R. \end{aligned}$$

$\forall i = 0, 1, \dots, n-1$: posons : $i + 1 = k$ alors : $i = k - 1$.

$$\begin{aligned} \text{On a donc : } \sum_{k=0}^n a_k X^k &= \sum_{k=1}^n b_{k-1} X^k - \sum_{k=0}^{n-1} \alpha b_k X^k + R \\ &= b_{n-1} X^n + \sum_{k=1}^{n-1} b_{k-1} X^k - \sum_{k=1}^{n-1} \alpha b_k X^k - \alpha b_0 + R \\ &= b_{n-1} X^n + \sum_{k=1}^{n-1} (b_{k-1} - \alpha b_k) X^k - \alpha b_0 + R. \end{aligned}$$

On a alors : $\begin{cases} a_n = b_{n-1} \\ \forall k = 1, 2, \dots, n-1 : a_k = b_{k-1} - \alpha b_k \\ a_0 = -\alpha b_0 + R \end{cases}$

Par suite on a :

$$\begin{cases} b_{n-1} = a_n \\ \forall k = 1, 2, \dots, n-1 : b_{k-1} = a_k + \alpha b_k \\ R = a_0 + \alpha b_0 \end{cases} \quad \text{c'est à dire} \quad \begin{cases} b_{n-1} = a_n \\ b_{n-2} = a_{n-1} + \alpha b_{n-1} \\ \dots \dots \dots \\ b_0 = a_1 + \alpha b_1 \\ R = a_0 + \alpha b_0 \end{cases}$$

Pratiquement pour déterminer les nombres $b_0, b_1, \dots, b_{n-1}$ et R on peut utiliser le tableau suivant appelé le procédé de Hôrner :

	a_n	a_{n-1}		a_1	a_0
α		αb_{n-1}		αb_1	αb_0
	$b_{n-1} = a_n$	$b_{n-2} = a_{n-1} + \alpha b_{n-1}$		$b_0 = a_1 + \alpha b_1$	$R = a_0 + \alpha b_0$

Exemple :

Dans $\mathbb{Z}$, soit $A = 2X^5 - 7X^4 + 5X^2 + 13X + 6$.

★ Pour effectuer la division euclidienne de A par $X - 3$ on peut utiliser le procédé de

Hörner suivant :

	2	-7	0	5	13	6
3		6	-3	-9	-12	3
	2	-1	-3	-4	1	9

on obtient le résultat suivant :

on obtient le résultat suivant :

$Q = 2X^4 - X^3 - 3X^2 - 4X + 1$ est le quotient de la division euclidienne de A par $X - 3$
 $R = A(3) = 9$ est le reste de la division euclidienne de A par $X - 3$.

★ Pour développer le polynôme A suivant les puissances de $X - \alpha$ on peut utiliser le procédé de Hôrner suivant :

	2	-7	0	5	13	6
3		6	-3	-9	-12	3
	2	-1	-3	-4	1	9
3		6	15	36	96	
	2	5	12	32	97	
3		6	33	135		
	2	11	45	167		
3		6	51			
	2	17	96			
3		6				
	2	23				
3						
	2					

Donc : $A = 9 + 97(X - 3) + 167(X - 3)^2 + 96(X - 3)^3 + 23(X - 3)^4 + 2(X - 3)^5$
est le développement de $A = 2X^5 - 7X^4 + 5X^2 + 13X + 6$ suivant les puissances de $X - 3$.

3-4-Divisibilité :

Définition 3-4-1 :

Soient A et B deux polynômes à coefficients dans K .

On dit que A divise B ou A est un diviseur de B ou B est un multiple de A et on note $A|B$ s'il existe un polynôme $Q \in K[X]$ tel que $B = AQ$. C'est à dire :

$$A|B \Leftrightarrow \exists Q \in K[X] \text{ tq : } B = AQ$$

Dans le cas contraire. C'est à dire si A ne divise pas B on note $A \nmid B$.

Propriétés 3-4-2 :

1) Si $K = \mathbb{C}$ alors : $\forall A, B \in K[X] : A|B \Rightarrow \bar{A}|\bar{B}$.

2) $\forall A, B \in K[X] : A|B \Leftrightarrow B \cdot K[X] \subset A \cdot K[X]$.

3) $\forall A \in K[X] : A|A$.

4) $\forall A, B \in K[X] : \begin{cases} A|B \\ B|C \end{cases} \Rightarrow A|C$.

5) Soient A, B, D et M des polynômes à coefficients dans K .

a) Pour que D soit un diviseur commun de A et B il faut et il suffit que $A \cdot K[X] + B \cdot K[X] \subset D \cdot K[X]$.

C'est à dire : $\begin{cases} D|A \\ D|B \end{cases} \Leftrightarrow A \cdot K[X] + B \cdot K[X] \subset D \cdot K[X]$.

b) Pour que M soit un multiple commun de A et B il faut et il suffit que $M \cdot K[X] \subset A \cdot K[X] \cap B \cdot K[X]$.

C'est à dire : $\begin{cases} A|M \\ B|M \end{cases} \Leftrightarrow M \cdot K[X] \subset A \cdot K[X] + B \cdot K[X]$.

c) Si D est un diviseur commun de A et B alors D est un diviseur commun de $A + B$ et $A - B$.

C'est à dire : $\begin{cases} D|A \\ D|B \end{cases} \Rightarrow \begin{cases} D|(A + B) \\ D|(A - B) \end{cases}$.

d) Si K est un corps commutatif de caractéristique différente de 2 alors :

D est un diviseur commun de A et B si et seulement si D est un diviseur commun de $A + B$ et $A - B$.

C'est à dire, si la caractéristique de K est différente de 2 alors :

$\begin{cases} D|A \\ D|B \end{cases} \Leftrightarrow \begin{cases} D|(A + B) \\ D|(A - B) \end{cases}$.

6) Soient $A \in K[X]$, $B \in K[X]^*$ de coefficient dominant inversible et si R est le reste de la division euclidienne de A par B .

Les diviseurs communs de A et B sont les diviseurs communs de B et R .

C'est à dire : $\forall D \in K[X] : \begin{cases} D|A \\ D|B \end{cases} \Leftrightarrow \begin{cases} D|B \\ D|R \end{cases}$

7) $\forall A \in K[X] : A|0$

C'est à dire que tous les polynômes à coefficients dans K sont des diviseurs de 0.

Ou encore 0 est un multiple commun à tous les polynômes à coefficients dans K .

- 8) $\forall A \in K[X] : 0|A \Leftrightarrow A = 0$. C'est à dire 0 est le seul multiple de 0.
- 9) $\forall A \in K[X]$ et $\forall \alpha \in U(K) : \alpha|A$
 C'est à dire les constantes inversibles de K sont des diviseurs communs à tous les polynômes à coefficients dans K . ou encore les polynômes à coefficients dans K sont des multiples communs à toutes les constantes inversibles de K .
- 10) Si K est un corps commutatif alors : $\forall \alpha \in K^* : \alpha|A$
 C'est à dire si K est un corps commutatif alors les constantes non nulles de K sont des diviseurs communs à tous les polynômes à coefficients dans K .
 Ou encore si K est un corps commutatif alors tous les polynômes à coefficients dans K sont des multiples communs à toutes les constantes non nulles de K .
- 11) Si α est une constante inversible alors : $\forall A \in K[X] : A|\alpha \Leftrightarrow A \in U(K[X])$.
 C'est à dire si K est intègre alors les seuls diviseurs d'une constante inversibles de K sont les polynômes inversibles de $K[X]$.
- 12) Si K est un corps commutatif et si α est une constante non nulle de K alors :
 $A|\alpha \Leftrightarrow A$ est une constante non nulle de K .
 C'est à dire si K est un corps commutatif alors les seuls diviseurs d'une constante non de K sont les constantes non nulles de K .
- 13) Si K est intègre alors : $\forall A, B \in K[X] : \begin{cases} A|B \\ B \neq 0 \end{cases} \Rightarrow d^0 A \leq d^0 B$.
- 14) Soient A et B deux un polynômes à coefficients dans K .
 a) Si $A \neq 0$ et si le coefficient dominant de B est inversible alors A est un diviseur de B si seulement si le reste de la division euclidienne de B par A est nul.
 b) Si A est unitaire alors A est un diviseur de B si seulement si le reste de la division euclidienne de B par A est nul.
 c) Si K est un corps commutatif et si $A \neq 0$ alors, A est un diviseur de B si et seulement si le reste de la division euclidienne de B par A est nul.
- 15) $\forall A \in K[X]$ et $\forall \alpha \in K : (X - \alpha)|A \Leftrightarrow A(\alpha) = 0$
 C'est à dire : $\forall A \in K[X]$ et $\forall \alpha \in K :$
 $X - \alpha$ est un diviseur de A si seulement si α est une racine de A .
- 16) On suppose que K est intègre et que A est un polynôme à coefficients dans K .
 a) Si $\alpha_1, \dots, \alpha_n$ sont des racines distinctes de A alors :

$$\prod_{k=1}^n (X - \alpha_k) = (X - \alpha_1)(X - \alpha_2) \dots (X - \alpha_n)$$
 est un diviseur de A .
 b) Le nombre des racines d'un polynôme non nul $A \in K[X]^*$ est fini et si r est le nombre des racines de A alors $r \leq d^0(A)$.
 c) Si A est un polynôme à coefficients dans K qui admet une infinité de racines dans K , alors A est nul.

Démonstration :

- 1) Supposons $K = \mathbb{C}$ et soient $A, B \in \mathbb{C}[X]$ tq : $A|B$.
 $A|B \Rightarrow \exists Q \in \mathbb{C}[X]$ tq : $B = AQ$. Alors : $\bar{B} = \overline{AQ} = \bar{A}\bar{Q} \Rightarrow \bar{A}|\bar{B}$.
- 2) Soient A et B deux polynômes quelconques à coefficients dans K .
 $\Rightarrow$ Si $A|B$:
 Alors il existe un polynôme $Q \in K[X]$ tel que $B = AQ$.
 $\forall M \in B \cdot K[X] : \exists N \in K[X]$ tq : $M = BN = AQN \in A \cdot K[X]$.
 $B \cdot K[X] \subset A \cdot K[X]$.

$\Leftrightarrow$ Si $B \cdot K[X] \subset A \cdot K[X]$:

$$B \in B \cdot K[X] \subset A \cdot K[X] \Rightarrow [\exists Q \in K[X] \text{ tq : } B = AQ] \Rightarrow A|B.$$

Donc : $A|B \Leftrightarrow B \cdot K[X] \subset A \cdot K[X]$.

3) $\forall A \in K[X] : A \cdot K[X] \subset A \cdot K[X] \Rightarrow A|A$.

4) $\forall A, B \in K[X] :$

$$\begin{cases} A|B \\ B|C \end{cases} \Rightarrow \begin{cases} B \cdot K[X] \subset A \cdot K[X] \\ C \cdot K[X] \subset B \cdot K[X] \end{cases} \Rightarrow C \cdot K[X] \subset B \cdot K[X] \Rightarrow A|C.$$

5) Soient A, B et D des polynômes à coefficients dans K .

$$a) \begin{cases} D|A \\ D|B \end{cases} \Leftrightarrow \begin{cases} A \cdot K[X] \subset D \cdot K[X] \\ B \cdot K[X] \subset D \cdot K[X] \end{cases} \Leftrightarrow A \cdot K[X] + B \cdot K[X] \subset D \cdot K[X].$$

$$b) \begin{cases} A|M \\ B|M \end{cases} \Leftrightarrow \begin{cases} M \cdot K[X] \subset A \cdot K[X] \\ A \cdot K[X] \subset B \cdot K[X] \end{cases} \Leftrightarrow M \cdot K[X] \subset A \cdot K[X] \cap B \cdot K[X].$$

c) Supposons que D soit un diviseur commun de A et B .

Il existe alors deux polynômes Q et R à coefficients dans K tels que :

$$\begin{cases} A = DQ \\ B = DR \end{cases}.$$

$$\text{Par suite on a : } \begin{cases} A + B = DQ + DR = D(Q + R) \\ A - B = DQ - DR = D(Q - R) \end{cases}.$$

Ce qui montre que D est un diviseur commun de $A + B$ et $A - B$.

d) Supposons que K est un corps commutatif de caractéristique différente de 2.

$\Rightarrow$ Si D est un diviseur commun de A et B :

Alors (d'après b)) D est un diviseur commun de $A + B$ et $A - B$.

$\Leftrightarrow$ Si D est un diviseur commun de $A + B$ et $A - B$:

Alors il existe deux polynômes Q et R à coefficients dans K tels que

$$\begin{cases} A + B = DQ \\ A - B = DR \end{cases}.$$

$$\text{Par suite on a : } \begin{cases} 2A = DQ + DR = D(Q + R) \\ 2B = DQ - DR = D(Q - R) \end{cases}$$

Puisque K est un corps de caractéristique différente de 2 alors :

$$\begin{cases} A = \frac{1}{2}D(Q + R) \\ B = \frac{1}{2}D(Q - R) \end{cases}.$$

Donc D est un diviseur commun de A et B .

Ce qui montre que D est un diviseur commun de A et B si et seulement si D est un diviseur commun de $A + B$ et $A - B$.

6) Soit Q le quotient de la division euclidienne de A par B . On a donc : $A = BQ + R$.

Soit D un polynôme quelconque à coefficients dans K .

⇒) **Si D est un diviseur commun de A et B :**

Alors il existe deux polynômes A_0 et B_0 tels que
$$\begin{cases} A = A_0 D \\ B = B_0 D \end{cases}.$$

Par suite on a : $A_0 D = B_0 D Q + R \Rightarrow R = A_0 D - B_0 D Q = (A_0 - B_0 Q) D \Rightarrow D | R$.

Donc D est un diviseur commun de B et R .

⇐) **Si D est un diviseur commun de B et R :**

Alors il existe deux polynômes B_0 et R_0 tels que
$$\begin{cases} B = B_0 D \\ R = R_0 D \end{cases}.$$

Par suite on a : $A = B_0 D Q + R_0 D = (B_0 Q + R_0) D \Rightarrow D | A$.

Donc D est un diviseur commun de A et B .

Ce qui montre que les diviseurs communs de A et B sont les diviseurs communs de B et R .

7) $\forall A \in K[X] : 0 \cdot K[X] = \{0\} \subset A \cdot K[X] \Rightarrow A | 0$.

8) $\forall A \in K[X] : 0 | A \Leftrightarrow A \cdot K[X] \subset 0 \cdot K[X] = \{0\} \Leftrightarrow A \cdot K[X] = \{0\} \Leftrightarrow A = 0$.

9) $\forall A \in K[X]$ et $\forall \alpha \in U(K) : A \cdot K[X] \subset K[X] = \alpha \cdot K[X] \Rightarrow \alpha | A$.

10) Si K est un corps commutatif alors : $\forall \alpha \in K^* : \alpha \in U(K) \Rightarrow \alpha | A$.

11) On suppose que α est une constante inversible.

Puisque $\alpha \in U(K)$ alors $\alpha \cdot K[X] = K[X]$.

Soit A un polynôme quelconque à coefficients dans K .

⇒) **Si A est un diviseur de α :**

Alors : $K[X] = \alpha \cdot K[X] \subset A \cdot K[X] \Rightarrow A \cdot K[X] = K[X] \Rightarrow 1 \in A \cdot K[X]$

Donc il existe $B \in K[X]$ tel que $AB = 1$ Ce qui prouve que $A \in U(K)$.

⇐) **Si $A \in U(K[X])$:**

Alors : $A \cdot K[X] = K[X] \Rightarrow \alpha \cdot K[X] \subset K[X] = A \cdot K[X] \Rightarrow A | \alpha$.

Donc : $A | \alpha \Leftrightarrow A \in U(K[X])$.

12) On suppose que K est un corps commutatif et que α est une constante non nulle de K .

$\forall A \in K[X] : A | \alpha \Leftrightarrow A \in U(K[X]) = U(K) = K^*$.

13) On suppose que K est intègre.

Soient A et B deux polynômes à coefficients dans K tels que B soit non nul et A soit un diviseur de B .

Alors il existe un polynôme Q à coefficients dans K tels $B = AQ$.

$B \neq 0 \Rightarrow AQ \neq 0 \Rightarrow [A \neq 0 \text{ et } Q \neq 0] \Rightarrow d^0 A, d^0 B, d^0 Q \in \mathbb{N}$.

Par suite on a : $d^0 A \leq d^0 A + d^0 Q = d^0 (AQ) = d^0 B$.

14) a) On suppose que $A \neq 0$ et que le coefficient dominant de B soit inversible.

Soient Q le quotient de la division euclidienne de B par A et R le reste de la division euclidienne de B par A .

⇒) **Si A est un diviseur de B :**

Alors il existe un polynôme D à coefficients dans K tels $B = AD$.

Par suite on a :
$$\begin{cases} B = AD + 0 \\ d^0 0 = -\infty < d^0 B \end{cases}.$$

Donc 0 est le reste de la division euclidienne de B par A .

Ce qui prouve que $R = 0$.

$\Leftrightarrow$) Si $R = 0$:

Alors : $B = AD + R = AD + 0 = AD \Rightarrow A|B$.

Ce qui montre que A est un diviseur de B si et seulement si le reste de la division euclidienne de B par A est nul.

b) et c) sont des cas particuliers de a).

15) $\forall A \in K[X]$ et $\forall \alpha \in K$: $A(\alpha)$ est le reste de la division euclidienne de A par $X - \alpha$.

Donc $(X - \alpha)|A \Leftrightarrow A(\alpha) = 0$.

16) a) On montre par récurrence sur $n \in \mathbb{N}^*$ que si $\alpha_1, \dots, \alpha_n$ sont des racines

distinctes de A alors : $\prod_{k=1}^n (X - \alpha_k)$ est un diviseur de A .

- Pour $n = 1$:

Si α_1 est une racine de A alors $\prod_{k=1}^1 (X - \alpha_k) = X - \alpha_1$ est un diviseur de A .

- Pour $n - 1$:

Supposons que si

- Pour n :

Montrons qu'alors, si $\alpha_1, \dots, \alpha_n$ sont des racines distinctes de A alors

$\prod_{k=1}^n (X - \alpha_k)$ est un diviseur de A .

Puisque $\alpha_1, \dots, \alpha_{n-1}$ sont des racines distinctes de A alors (d'après l'hypothèse de récurrence) il existe un polynôme Q à coefficients dans K tel

$$A = \prod_{k=1}^{n-1} (X - \alpha_k) Q.$$

Comme α_n est une racine de A alors $A(\alpha_n) = 0$.

$$\text{On a donc : } \left[\prod_{k=1}^{n-1} (X - \alpha_k) Q \right] (\alpha_n) = 0 \Rightarrow \left[\prod_{k=1}^{n-1} (\alpha_n - \alpha_k) \right] Q(\alpha_n) = 0.$$

Puisque A est intègre et puisque $\prod_{k=1}^{n-1} (\alpha_n - \alpha_k) \neq 0$ alors $Q(\alpha_n) = 0$.

Par suite il existe un polynôme S à coefficients dans K tel $Q = (X - \alpha_n)S$.

$$\text{Alors : } A = \prod_{k=1}^{n-1} (X - \alpha_k) Q = \left[\prod_{k=1}^{n-1} (X - \alpha_k) \right] (X - \alpha_n) S = \prod_{k=1}^n (X - \alpha_k) S.$$

Ce qui montre que $\prod_{k=1}^n (X - \alpha_k)$ est un diviseur de A .

b) Soit A un polynôme non nul à coefficients dans K et posons $d^0(A)$.

$A \neq 0 \Rightarrow n \in \mathbb{N}$.

Supposons que A admet au moins $n + 1$ racines $\alpha_1, \dots, \alpha_{n+1} \in K$.

Alors (d'après a)) $\prod_{k=1}^{n+1} (X - \alpha_k)$ est un diviseur de A .

D'après la propriété 13) on a : $d^0 \left(\prod_{k=1}^{n+1} (X - \alpha_k) \right) \leq d^0(A) = n$.

Par suite on a : $n + 1 = d^0 \left(\prod_{k=1}^{n+1} (X - \alpha_k) \right) \leq n$. Ce qui est absurde.

Donc le nombre des racines de A est fini et si r est le nombre des racines de A alors $r \leq d^0(A) = n$.

c) Soit A un polynôme à coefficients dans K qui admet une infinité de racines dans K .

D'après la contraposée de la propriété b) le polynôme A est nul.

3-5-Polynômes associés :

Définition 3-5-1 :

Soient A et B deux polynômes à coefficients dans K .

On dit que A est associé à B ou A et B sont associés et on note $A \sim B$ si A divise B et si

$$B \text{ divise } A. \text{ C'est à dire : } A \sim B \Leftrightarrow \begin{cases} A|B \\ B|A \end{cases}.$$

Propriétés 3-5-2 :

Soient A , B et C des polynômes à coefficients dans K .

- 1) Si $K = \mathbb{C}$ alors : $A \sim B \Rightarrow \bar{A} \sim \bar{B}$.
- 2) $A \sim B \Leftrightarrow A \cdot K[X] = B \cdot K[X]$.
- 3) $A \sim A$.
- 4) $A \sim B \Leftrightarrow B \sim A$.
- 5) $\begin{cases} A \sim B \\ B \sim C \end{cases} \Rightarrow A \sim C$.
- 6) $A \sim 0 \Leftrightarrow A = 0$.
C'est à dire 0 est le seul polynôme à coefficients dans K associé à 0.
- 7) Si K est intègre alors : $A \sim B \Leftrightarrow \exists \alpha \in U(K) \text{ tq : } B = \alpha A$.
- 8) Si K est un corps commutatif alors : $A \sim B \Leftrightarrow \exists \alpha \in K^* \text{ tq : } B = \alpha A$.
- 9) Si K est intègre et si A et B sont unitaires alors : $A \sim B \Rightarrow A = B$.
- 10) Si K est intègre et si A non nul de coefficient dominant $\alpha \in U(K)$ alors :
 $\alpha^{-1}A$ est le seul polynôme unitaire associé à A .
- 11) Si K est intègre et si A est non nul de coefficient dominant inversible alors A est associé à un polynôme unitaire et un seul.
- 12) Si K est un corps commutatif et si A est non nul de coefficient dominant α alors,
 $\alpha^{-1}A$ est le seul polynôme unitaire associé à A .
- 13) Si K est un corps commutatif et si A est non nul alors A est associé à un polynôme unitaire et un seul.
- 14) Si K est intègre et si $\alpha \in U(K)$ alors A est associé à α si et seulement si $A \in U(K)$.
C'est à dire si K est intègre et si $\alpha \in U(K)$ alors : $A \sim \alpha \Leftrightarrow A \in U(K)$.
- 15) Si K est un corps commutatif et si α est un élément non nul de K alors A est associé à α si et seulement si $A \in K^*$.
C'est à dire si K est un corps commutatif et si $\alpha \in K^*$ alors : $A \sim \alpha \Leftrightarrow A \in K^*$.
- 16) Si K est intègre alors : $A \sim 1 \Leftrightarrow A \in U(K)$.
- 17) Si K est un corps commutatif alors : $A \sim 1 \Leftrightarrow A \in K^*$.

- 18) Si K est intègre et si A est associé à B alors $d^0 A = d^0 B$.
 19) Si K est un corps commutatif et si A est un diviseur de B alors :
 $A \sim B \Leftrightarrow d^0 A = d^0 B$

Démonstration :

- 1) Supposons que $K = \mathbb{C}$.
 $A \sim B \Rightarrow [A|B \text{ et } B|A] \Rightarrow [\bar{A}|\bar{B} \text{ et } \bar{B}|\bar{A}] \Rightarrow \bar{A} \sim \bar{B}$.
- 2) $A \sim B \Leftrightarrow [A|B \text{ et } B|A] \Leftrightarrow [A \cdot K[X] \subset B \cdot K[X] \text{ et } B \cdot K[X] \subset A \cdot K[X]]$
 $\Leftrightarrow A \cdot K[X] = B \cdot K[X]$.
- 3) $A \cdot K[X] = A \cdot K[X] \Rightarrow A \sim A$.
- 4) $A \sim B \Leftrightarrow A \cdot K[X] = B \cdot K[X] \Leftrightarrow B \cdot K[X] = A \cdot K[X] \Leftrightarrow B \sim A$.
- 5) Supposons que A est associé à B et que B est associé à C .

$$\begin{cases} A \sim B \\ B \sim C \end{cases} \Rightarrow \begin{cases} A \cdot K[X] = B \cdot K[X] \\ B \cdot K[X] = C \cdot K[X] \end{cases} \Rightarrow A \cdot K[X] = C \cdot K[X] \Rightarrow A \sim C$$
.
- 6) $A \sim 0 \Leftrightarrow A \cdot K[X] = 0 \cdot K[X] = \{0\} \Leftrightarrow A = 0$.
- 7) Supposons que K est intègre.
 $\Rightarrow$) **Si A est associé à B :**
 - **Si A est nul :**
 Alors (d'après 6)) B est nul. Il suffit de prendre $\alpha = 1$
 Donc $\alpha = 1 \in U(K)$ et $B = 0 = 1 \times 0 = \alpha A$.
 - **Si A est non nul :**
 Alors : $\begin{cases} A|B \\ B|A \end{cases} \Rightarrow \exists P, Q \in K[X] \quad tq : \begin{cases} B = PA \\ A = QB \end{cases}$.
 Donc : $A = QB = QPA \Rightarrow QP = 1 \Rightarrow P \in U(K[X])$.
 Puisque K est intègre, il existe $\alpha \in K$ tel que $P = \alpha \in U(K)$.
 Ce qui montre que $\alpha \in U(K)$ et $B = \alpha A$.
 $\Leftarrow$) **S'il existe $\alpha \in U(K)$ tel que : $B = \alpha A$:**
 Alors : $\begin{cases} B = \alpha A \\ A = \alpha^{-1} B \end{cases} \Rightarrow \begin{cases} A|B \\ B|A \end{cases} \Rightarrow A \sim B$.
- 8) Supposons que K est un corps commutatif.
 Alors : $U(K) = K^*$.
 Donc : $A \sim B \Leftrightarrow \exists \alpha \in U(K) = K^* \quad tq : B = \alpha A$.
- 9) Supposons que K est intègre et que A et B sont unitaires associés.
 Alors : $\exists \alpha \in U(K) \quad tq : B = \alpha A$.
 Puisque A est unitaire alors α est le coefficient dominant de B .
 Par suite $\alpha = 1$ (car B est unitaire).
 Donc : $A = B$.
- 10) Supposons que K est intègre et que A est non nul de coefficient dominant $\alpha \in U(K)$.
 * $\alpha^{-1}A$ est de coefficient dominant $\alpha^{-1}\alpha = 1$.
 Donc $\alpha^{-1}A$ est un polynôme à coefficient dans K unitaire associé à A .
 * Soit B un polynôme à coefficient dans K unitaire quelconque associé à A .
 D'après 7) il existe un élément β de $U(K)$ tel que $B = \beta A$.
 $\beta\alpha$ est le coefficient dominant de B . Alors : $\beta\alpha = 1$ (car B est unitaire).
 Donc : $\beta = \alpha^{-1}$, et par suite $B = \alpha^{-1}A$.
 Ce qui montre que $\alpha^{-1}A$ est le seul polynôme unitaire associé à A .

- 11) Supposons que K est intègre et que A est non nul de coefficient dominant inversible.
Soit α le coefficient dominant de A .
D'après 10) $\alpha^{-1}A$ est le seul polynôme unitaire associé à A .
- 12) Supposons que K est un corps commutatif et que A est non nul de coefficient dominant α .
Puisque K est un corps commutatif alors $\alpha \in K^* = U(K)$
Donc (d'après 10)) $\alpha^{-1}A$ est le seul polynôme unitaire associé à A .
- 13) Supposons que K est un corps commutatif et que A est non nul.
Puisque K est un corps commutatif alors le coefficient dominant de A est inversible.
Ce qui montre (d'après 11)) que A est associé à un polynôme unitaire et un seul.
- 14) Supposons que K est intègre et que $\alpha \in U(K)$
 $\Rightarrow$) **Si A est associé à α :**
Alors (d'après 7)) il existe une constante $\beta \in U(K)$ telle que $A = \beta\alpha$.
Donc $A = \beta\alpha \in U(K)$.
 $\Leftarrow$) **Si $A \in U(K)$:**
Alors : $\alpha A^{-1} \in U(K)$ et $\alpha = (\alpha A^{-1})A$.
Ce qui montre (d'après 7)) que A est associé à α .
- 15) Supposons que K est un corps commutatif et que α est un élément non nul de K .
Puisque K est un corps commutatif alors $\alpha \in U(K)$
D'après 14), on a donc : $A \sim \alpha \Leftrightarrow A \in U(K) = K^*$.
- 16) Supposons que K est intègre.
Puisque $1 \in U(K)$ alors (d'après 14)) $A \sim 1 \Leftrightarrow A \in U(K)$.
- 17) Supposons que K est un corps commutatif.
D'après 16), on a donc : $A \sim 1 \Leftrightarrow A \in U(K) = K^*$.
- 18) Supposons que K est intègre et que A est associé à B .
- **Si A est nul :**
Alors B est aussi nul. Donc : $d^0 A = d^0 0 = d^0 B$.
- **Si A est non nul :**
Alors B est aussi non nul. On a donc :
$$\begin{cases} A|B \\ B|A \end{cases} \Rightarrow \begin{cases} d^0 A \leq d^0 B \\ d^0 B \leq d^0 A \end{cases} \Rightarrow d^0 A = d^0 B$$
- 19) Supposons que K est un corps commutatif et que A est un diviseur de B .
 $\Rightarrow$) **Si A est associé à B :**
Alors (d'après 18)) $d^0 A = d^0 B$
 $\Leftarrow$) **Si $d^0 A = d^0 B$:**
- **Si A est nul :**
Alors : $d^0 B = d^0 A = d^0 0 = -\infty \Rightarrow B = 0$.
Donc : $A = 0 \sim 0 = B$.
- **Si A est non nul :**
 $A|B \Rightarrow \exists Q \in K[X] \text{ tq : } B = AQ$.
 $d^0 A + d^0 Q = d^0(AQ) = d^0 B = d^0 A \Rightarrow d^0 Q = 0 \Rightarrow Q \in K^* = U(K)$.
Donc (d'après 7)) A est associé à B .

Thorème 3-5-3 :

Si K est un anneau commutatif unitaire intègre non nul, les trois propriétés suivantes sont équivalentes :

- i) K est un corps commutatif.
- ii) $K[X]$ est un anneau euclidien.
- iii) $K[X]$ est un anneau principal.

Démonstration :

i) $\Rightarrow$ ii) Supposons que K est un corps commutatif.

Soit d l'application de $K[X]^*$ vers $\mathbb{N}$ définie par : $d : K[X]^* \rightarrow \mathbb{N}$
 $A \mapsto d(A) = d^0 A.$

$$\forall A \in K[X] \text{ et } \forall B \in K[X]^* : \exists Q, R \in K[X] \text{ tq : } \begin{cases} A = BQ + R \\ d^0 R < d^0 B \end{cases} ;$$

$$\text{Alors : } \begin{cases} A = BQ + R \\ R = 0 \text{ ou } [R \neq 0 \text{ et } d(R) = d^0 R < d^0 B = d(B)] \end{cases} .$$

Donc $K[X]$ est un anneau euclidien.

Ce qui montre que la proposition i) $\Rightarrow$ ii) est vraie.

ii) $\Rightarrow$ iii) Supposons que $K[X]$ est un anneau euclidien.

Alors $K[X]$ est un anneau principal.

Donc la proposition ii) $\Rightarrow$ iii) est vraie.

iii) $\Rightarrow$ i) Supposons que $K[X]$ est un anneau principal.

Soit a un élément quelconque non nul K .

Puisque $K[X]$ est un anneau principal alors l'idéal $a \cdot K[X] + X \cdot K[X]$ est principal.

Donc il existe un polynôme $d \in K[X]$ tel que : $a \cdot K[X] + X \cdot K[X] = d \cdot K[X].$

$a \cdot K[X] \subset a \cdot K[X] + X \cdot K[X] = d \cdot K[X] \Rightarrow d|a \Rightarrow d^0(d) \leq d^0(a) = 0 \Rightarrow d \in K.$

$[d|a \text{ et } a \neq 0] \Rightarrow d \neq 0. \text{ Donc : } d \in K^*.$

$X \cdot K[X] \subset a \cdot K[X] + X \cdot K[X] = d \cdot K[X] \Rightarrow d|X \Rightarrow \exists P \in K[X] \text{ tq : } X = dP.$

$dP = X \Rightarrow d^0 P = 0 + d^0 P = d^0(d) + d^0 P = d^0(dP) = d^0 X = 1.$

Alors : $\exists \alpha, \beta \in K \text{ tq : } P = \alpha X + \beta.$

$dP = X \Rightarrow d(\alpha X + \beta) = X \Rightarrow d\alpha X + d\beta = X \Rightarrow d\alpha = 1 \Rightarrow d \in U(K)$

$\Rightarrow d \cdot K[X] = K[X].$

Par suite on a : $a \cdot K[X] + X \cdot K[X] = d \cdot K[X] = K[X] \Rightarrow 1 \in a \cdot K[X] + X \cdot K[X].$

Donc il existe $U, V \in K[X]$ tels que : $Ua + VX = 1.$

$Ua + VX = 1 \Rightarrow (Ua + VX)(0) = 1(0) = 1 \Rightarrow U(0)a + V(0)(0) = 1 \Rightarrow U(0)a = 1$
 $\Rightarrow a \in U(K).$

Ce qui montre que K est un corps commutatif.

Alors la proposition iii) $\Rightarrow$ i) est vraie.

On a donc montré que les trois propositions i), ii) et iii) sont équivalentes.

3-6-Fonctions polynômiales :

Définition 3-6-1 :

Soient A un polynôme à coefficients dans K .

On appelle fonction polynômiale associé à A l'application de K vers K noté $\tilde{A}$ appelée

" A tilda" définie par : $\tilde{A} : K \rightarrow K$
 $x \mapsto \tilde{A}(x) = A(x).$

Définition 3-6-2 :

Soit $u \in K^K$ une application de K vers K lui même .

S'il existe un polynôme A à coefficients dans K tel que $u = \tilde{A}$ on dit que u est une fonction polynômiale de K ou u est une fonction polynômiale.

Remarque 3-6-3 :

$$\forall A, B \in K[X] : \begin{cases} \widetilde{A+B} = \tilde{A} + \tilde{B} \\ \widetilde{AB} = \tilde{A}\tilde{B} \end{cases}.$$

En effet :

$\forall A, B \in K[X]$ et $\forall x \in K :$

$$\begin{cases} \widetilde{A+B}(x) = (A+B)(x) = A(x) + B(x) = \tilde{A}(x) + \tilde{B}(x) = (\tilde{A} + \tilde{B})(x) \\ \widetilde{AB}(x) = (AB)(x) = A(x)B(x) = \tilde{A}(x)\tilde{B}(x) = (\tilde{A}\tilde{B})(x) \end{cases}.$$

$$\text{On a donc : } \begin{cases} \widetilde{A+B} = \tilde{A} + \tilde{B} \\ \widetilde{AB} = \tilde{A}\tilde{B} \end{cases}.$$

Propriétés 3-6-4 :

K étant un anneau commutatif unitaire intègre non nul.

Soit φ l'application de $K[X]$ vers l'ensemble K^K des applications de K vers K lui même définie par : $\varphi : K[X] \rightarrow K^K$

$$A \mapsto \varphi(A) = \tilde{A}$$

Pour tout entier naturel n , la restriction de φ à $K_n[X]$ est notée φ_n . C'est à dire, pour tout entier naturel n , l'application φ_n est définie par :

$$\varphi_n : K_n[X] \rightarrow K^K$$

$$A \mapsto \varphi_n(A) = \varphi(A) = \tilde{A}$$

1) φ est un homomorphisme d'anneaux unitaires de $K[X]$ vers l'anneau K^K des applications de K vers K lui même.

2) $\ker \varphi = \{A \in K[X] \quad tq : \forall x \in K : A(x) = 0\}.$

3) Pour que φ soit injectif il faut et il suffit que K soit infini.

4) Si K est infini alors l'application suivante : $u : K \rightarrow K$

$$x \mapsto u(x) = 0 \quad \text{si } x \neq 0$$

$$0 \mapsto u(0) = 1 \quad \text{si } x = 0$$

de K vers K n'est pas une fonction polynômiale dans K .

5) Si K est infini alors l'homomorphisme φ n'est pas surjectif.

- 6) Si K est infini alors $K[X]$ est isomorphe à un sous anneau propre de K^K .
- 7) Pour tout entier naturel n , l'application φ_n est un homomorphisme du groupe additif $(K_n[X], +)$ vers le groupe additif $(K^K, +)$.
- 8) Si K est infini alors, pour tout entier naturel n , φ_n est injectif.
- 9) Si K est fini alors, pour tout entier naturel n , φ_n est injectif si et seulement si $n < |K|$.
C'est à dire si K est fini alors, pour tout entier naturel n , φ_n est injectif $\Leftrightarrow n < |K|$.
- 10) Si K est fini et si $|K| = n + 1$ alors φ_n est un isomorphisme du groupe additif $(K_n[X], +)$ vers le groupe additif $(K^K, +)$.
- 11) Si K est fini alors l'homomorphisme φ est surjectif.
- 12) Si K est fini alors : $\prod_{a \in K} (X - a) \in \ker \varphi - \{0\}$.
- 13) Si K est fini alors l'homomorphisme φ n'est pas injectif.

Démonstration :

$$1) \star \forall A, B \in K[X] : \begin{cases} \varphi(A + B) = \widetilde{A + B} = \widetilde{A} + \widetilde{B} = \varphi(A) + \varphi(B) \\ \varphi(AB) = \widetilde{AB} = \widetilde{A} \widetilde{B} = \varphi(A) \varphi(B) \end{cases}.$$

Donc φ est un homomorphisme d'anneaux de $K[X]$ vers K^K

$$\star \forall x \in K : \varphi(1)(x) = \widetilde{1}(x) = 1(x) = 1.$$

Donc $\varphi(1)$ est égal à la constante 1 de K .

Ce qui montre que φ est un homomorphisme d'anneaux unitaires de $K[X]$ vers K^K .

Car l'unité K^K est égal à la constante 1 de K .

$$2) \forall A \in K[X] : A \in \ker \varphi \Leftrightarrow \widetilde{A} = \varphi(A) \text{ est nul} \Leftrightarrow [\forall x \in K : A(x) = \widetilde{A}(x) = 0].$$

$$\text{Donc : } \ker \varphi = \{A \in K[X] \mid \forall x \in K : A(x) = 0\}.$$

3) $\Rightarrow$) **Si φ est injectif :**

Supposons que K est fini et posons $A = \prod_{a \in K} (X - a)$. Le polynôme A est non nul.

$$\left[\forall x \in K : A(x) = \prod_{a \in K} (x - a) = 0 \right] \Rightarrow A \in \ker \varphi. \text{ Donc } \ker \varphi \text{ est non nul.}$$

Alors φ n'est pas injectif, ce qui est absurde. Ce qui prouve que K soit infini.

$\Leftarrow$) **Si K est infini :**

$\forall A \in \ker \varphi : \forall x \in K : A(x) = 0$. Donc les éléments de K sont tous des racines de A . Alors A admet une infinité de racines dans K et par suite A est nul.

Donc $\ker \varphi$ est nul. Ce qui montre que φ est injectif.

4) Supposons que K est infini.

Les racines de u dans K sont les éléments de K^* .

Puisque K est infini alors K^* est aussi infini et donc u admet une infinité de racines dans K . Ce qui montre que u n'est pas une fonction polynômiale dans K .

5) Supposons que K est infini.

Alors (d'après 4)) il existe un élément $u \in K^K$ tel que u ne soit pas une fonction polynômiale dans K .

$$\text{On donc : } \forall A \in K[X] : \varphi(A) \neq u.$$

Ce qui prouve que φ n'est pas surjectif.

6) Supposons que K est infini.

Alors φ est un isomorphisme de $K[X]$ vers $\varphi(K[X]) \neq K^K$ (car φ n'est pas surjectif).

Donc $K[X]$ est isomorphe à un sous anneau propre de K^K .

- 7) $\forall A, B \in K_n[X] : \varphi_n(A + B) = \varphi(A + B) = \varphi(A) + \varphi(B) = \varphi_n(A) + \varphi_n(B)$.
Donc φ_n est un homomorphisme du groupe additif $(K_n[X], +)$ vers le groupe additif $(K^K, +)$.
- 8) Supposons que K est infini et soit n entier nature quelconque.
 $\forall A \in \ker \varphi_n : \varphi(A) = \varphi_n(A) = \theta$ (où θ est l'application nulle de K vers K lui même).
Donc $A = 0$.
Alors $\ker \varphi_n$ est nul. Ce qui montre que φ_n est injectif.
- 9) Supposons que K est fini et soit n entier nature quelconque. Posons $|K| = m$.
 $\Rightarrow$) **Si φ_n est injectif :**
Supposons que $n \geq |K| = m$ et soit $A = \prod_{a \in K} (X - a) \in K[X]$.
 $d^0 A = |K| = m \leq n \Rightarrow A \in K_n[X]^*$ et on a : $\forall x \in K : A(x) = \prod_{a \in K} (x - a) = 0$.
Alors pour tout élément x de K , $\varphi_n(A)(x) = \varphi(A)(x) = A(x) = 0$.
Donc $\varphi_n(A)$ est nul et par suite $A \in \ker \varphi_n$. Ce qui prouve que φ_m n'est pas injectif. Ce qui est absurde.
Par conséquent $n < m = |K|$.
- $\Leftarrow$) **Si $n < |K|$:**
Soit A un élément quelconque de $\ker \varphi_n$.
On a : $A \in \ker \varphi_n \subset K_n[X] \Rightarrow d^0 A \leq n < m$.
 $\forall x \in K : A(x) = \tilde{A}(x) = \varphi(A)(x) = \varphi_n(A)(x) = \theta(x) = 0$, où θ est l'application nulle de K vers K lui même.
Puisque $d^0 A < m$ et puisque A admet m racines dans K distincts deux à deux alors A est nul.
Donc $\ker \varphi_n$ est nul, ce qui montre que φ_n est injectif.
- 10) Supposons que K est d'ordre fini $n + 1$.
Puisque $n < n + 1 = |K|$ alors (d'après 9)) est injectif. Donc φ_n est un isomorphisme du groupe additif $(K_n[X], +)$ vers le groupe additif $(\varphi_n(K_n[X]), +)$.
 $|\varphi_n(K_n[X])| = |K_n[X]| = |K|^{n+1} = (n + 1)^{n+1} = |K|^{|K|} = |K^K|$.
Par conséquent $\varphi_n(K_n[X]) = K^K$. Alors φ_n est surjectif.
Ce qui montre que φ_n est un isomorphisme du groupe additif $(K_n[X], +)$ vers le groupe additif $(K^K, +)$.
- 11) Supposons que K est fini et posons $|K| - 1 = n$.
Alors φ_n est un isomorphisme du groupe additif $(K_n[X], +)$ vers le groupe additif $(K^K, +)$.
Donc $K^K = \varphi_n(K_n[X]) = \varphi(K_n[X]) \subset \varphi(K[X]) \Rightarrow \varphi(K[X]) = K^K$.
Ce qui montre que l'homomorphisme φ est surjectif.
- 12) Supposons que K est fini.
$$d^0 \left(\prod_{a \in K} (X - a) \right) = |K| \neq -\infty \Rightarrow \prod_{a \in K} (X - a) \neq 0.$$

On a a : $\left[\forall x \in K : \left[\prod_{a \in K} (X - a) \right] (x) = \prod_{a \in K} (x - a) = 0 \right]$.
Donc $\prod_{a \in K} (X - a) \in \ker \varphi - \{0\}$.
- 13) Supposons que K est fini.
Puisque (d'après 12) $\prod_{a \in K} (X - a) \in \ker \varphi - \{0\}$ alors φ n'est pas injectif.

Théorème 3-6-5 :

Soit K est un anneau commutatif unitaire intègre non nul. Les propriétés suivantes sont vérifiées :

- 1) Si K est infini alors $K[X]$ est isomorphe à un sous anneau propre de K^K .
- 2) Si K est infini alors :
 - $\forall A \in K[X] : \tilde{A} = \theta \Rightarrow A = 0$ (où θ est l'application nulle K vers K lui-même).
 - $\forall A, B \in K[X] : \tilde{A} = \tilde{B} \Rightarrow A = B$.
- 3) Si K est infini alors les applications de K vers K lui-même ne sont pas toutes des fonctions polynômiales de K .
- 4) Si K est infini, tout polynôme A à coefficients dans K peut être confondu avec la fonction polynômiale $\tilde{A}$.
- 5) Si K est fini alors toutes les applications de K vers K sont des fonctions polynômiales de K . C'est à dire : $\forall u \in K^K : \exists A \in K[X] \text{ tq } : u = \tilde{A}$.
- 6) Si K est fini alors :
 - $\forall A \in K[X] : \tilde{A} = \theta \nRightarrow A = 0$ (où θ est l'application nulle K vers K lui-même).
 - $\forall A, B \in K[X] : \tilde{A} = \tilde{B} \nRightarrow A = B$.

Démonstration :

Soit φ l'homomorphisme de $(K[X], +, \cdot)$ vers $(K^K, +, \cdot)$ défini par : $\varphi : K[X] \rightarrow K^K$
 $A \mapsto \varphi(A) = \tilde{A}$.

- 1) Supposons que K est infini.
 D'après la propriété 3-6-6-6) $K[X]$ est isomorphe à un sous anneau propre de K^K .
- 2) Supposons que K est infini.
 D'après la propriété 3-6-6-3) φ est injectif. Par suite on a :
 - $\forall A \in K[X] : \tilde{A} = \theta \Rightarrow \varphi(A) = \theta \Rightarrow A = 0$.
 - $\forall A, B \in K[X] : \tilde{A} = \tilde{B} \Rightarrow \varphi(A) = \varphi(B) \Rightarrow A = B$.
- 3) Supposons que K est infini.
 D'après la propriété 3-6-6-5) les applications de K vers K lui-même ne sont pas toutes des fonctions polynômiales de K .
- 4) Supposons que K est infini.
 Puisque d'après la propriété 3-6-6-3) φ est un homomorphisme injectif de $(K[X], +, \cdot)$ vers $(K^K, +, \cdot)$, on peut confondre chaque polynôme A à coefficients dans K avec la fonction polynômiale $\tilde{A}$.
- 5) Supposons que K est fini.
 Puisque d'après la propriété 3-6-6-11) φ est un homomorphisme surjectif de $(K[X], +, \cdot)$ vers $(K^K, +, \cdot)$ alors : $\forall u \in K^K : \exists A \in K[X] \text{ tq } : u = \varphi(A) = \tilde{A}$.
 Donc toutes les applications de K vers K sont des fonctions polynômiales de K .
- 6) Supposons que K est fini.
 Puisque d'après la propriété 3-6-6-13) φ n'est pas injectif alors :
 - $\forall A \in K[X] : \tilde{A} = \theta \Rightarrow \varphi(A) = \theta \nRightarrow A = 0$.
 - $\forall A, B \in K[X] : \tilde{A} = \tilde{B} \Rightarrow \varphi(A) = \varphi(B) \nRightarrow A = B$.

3-7-Division suivant les puissances croissantes :

Lemme 3-7-1 :

Soient A et B deux polynômes à coefficients dans K .

Si le coefficient constant $B(0)$ de B est inversible (c'est à dire si $B(0) \in U(K)$) alors il existe d'une façon unique un élément α de K et un polynôme R à coefficients dans K tels que $A = \alpha B + XR$.

Démonstration :

Supposons que le coefficient constant de B est inversible.

- Existence :

Posons $\alpha = A(0)B(0)^{-1}$ On alors :

$$(A - \alpha B)(0) = A(0) - \alpha B(0) = A(0) - A(0)B(0)^{-1}B(0) = A(0) - A(0) = 0.$$

Alors : $X|(A - \alpha B) \Rightarrow \exists R \in K[X] \text{ tq : } A - \alpha B = XR.$

Donc il existe un élément α de K et un polynôme R à coefficients dans K tels que $A = \alpha B + XR$.

- Unicité :

Soient β un élément de K et S un polynôme à coefficients dans K tels que $A = \beta B + XS$.

Alors : $\alpha B + XR = A = \beta B + XS \Rightarrow \alpha B - \beta B = XS - XR \Rightarrow (\alpha - \beta)B = X(S - R)$

$$\Rightarrow [(\alpha - \beta)B](0) = [X(S - R)](0)$$

$$\Rightarrow (\alpha - \beta)B(0) = 0(S - R)(0) = 0$$

$$\Rightarrow (\alpha - \beta)B(0)B(0)^{-1} = 0B(0)^{-1} = 0 \Rightarrow \alpha - \beta = 0$$

$$\Rightarrow \alpha = \beta.$$

Par suite on a : $\alpha B + XR = A = \beta B + XS = \alpha B + XS \Rightarrow XR = XS \Rightarrow R = S.$

On a donc : $\alpha = \beta$ et $R = S$. D'où l'unicité.

Théorème et définition 3-7-2 :

Soient A et B deux polynômes à coefficients dans K .

Si le coefficient constant de B est inversible (c'est à dire si $B(0) \in U(K)$)

alors pour tout entier naturel $n \in \mathbb{N}$ il existe d'une façon unique deux polynômes Q et R à coefficients dans K tels que :

$$\begin{cases} A = BQ + X^{n+1}R \\ d^0 Q \leq n \end{cases}.$$

Le polynôme Q est appelé le quotient de la division suivant les puissances croissantes de A par B à l'ordre n ou Q est le quotient de A par B à l'ordre n .

Le polynôme $X^{n+1}R$ est appelé le reste de la division suivant les puissances croissantes de A par B à l'ordre n ou le reste de A par B à l'ordre n .

La recherche des polynômes Q et R est appelée la division suivant les puissances croissantes de A par B à l'ordre n ou la division de A par B à l'ordre n .

Démonstration :

Supposons que le coefficient constant de B est inversible.

Montrons par récurrence que pour tout entier naturel n il existe d'une façon unique deux

polynômes Q et R à coefficients dans K tels que : $\begin{cases} A = BQ + X^{n+1}R \\ d^0 Q \leq n \end{cases}.$

- **Pour $n = 0$:**

D'après le lemme 3-7-1, il existe d'une façon unique un élément α de K et un polynôme R à coefficients dans K tels que $A = \alpha B + XR$.

- **Existence :**

$$\text{Posons } Q = \alpha. \text{ On a alors : } \begin{cases} A = \alpha B + XR = BQ + X^{n+1}R \\ d^0 Q = d^0 \alpha \leq 0 = n \end{cases}.$$

D'où l'existence.

- **Unicité :**

$$\text{Soient } M \text{ et } S \text{ deux polynômes à coefficients dans } K \text{ tels que : } \begin{cases} A = BM + X^{n+1}S \\ d^0 M \leq n \end{cases}.$$

$$d^0 M \leq n = 0 \Rightarrow \exists \beta \in K \text{ tq : } d^0 M = \beta.$$

$$\text{On a donc : } \begin{cases} A = BQ + X^{n+1}R = \alpha B + XR \\ A = BM + X^{n+1}S = \beta B + XS \end{cases}.$$

$$\text{D'après le lemme 3-7-1 on a : } \begin{cases} Q = \alpha = \beta = M \\ R = S \end{cases}.$$

D'où l'unicité.

- **Pour $n - 1$:**

Supposons qu'il existe d'une façon unique deux polynômes Q_0 et A_0 à coefficients dans

$$K \text{ tels que : } \begin{cases} A = BQ_0 + X^n A_0 \\ d^0 Q_0 \leq n - 1 \end{cases}.$$

- **Pour n :**

Montrons qu'alors il existe d'une façon unique deux polynômes Q et R à coefficients

$$\text{dans } K \text{ tels que : } \begin{cases} A = BQ + X^n R \\ d^0 Q \leq n \end{cases}.$$

• **Existence :**

D'après l'hypothèse de récurrence il existe d'une façon unique deux polynômes Q_0 et

$$A_0 \text{ à coefficients dans } K \text{ tels que : } \begin{cases} A = BQ_0 + X^n A_0 \\ d^0 Q_0 \leq n - 1 \end{cases}.$$

D'après le lemme 3-7-1, il existe d'une façon unique un élément α de K et un polynôme R à coefficients dans K tels que $A_0 = \alpha B + XR$.

$$\text{Alors : } A = BQ_0 + X^n(\alpha B + XR) = BQ_0 + \alpha BX^n + X^{n+1}R = B(Q_0 + \alpha X^n) + X^{n+1}R.$$

$$\text{Posons } Q = Q_0 + \alpha X^n. \text{ Puisque } d^0 Q_0 \leq n - 1 \text{ alors : } d^0 Q = d^0(Q_0 + \alpha X^n) \leq n.$$

$$\text{On a donc : } \begin{cases} A = BQ + X^{n+1}R \\ d^0 Q \leq n \end{cases}.$$

D'où l'existence.

• **Unicité :**

$$\text{Soient } M \text{ et } S \text{ deux polynômes à coefficients dans } K \text{ tels que : } \begin{cases} A = BM + X^{n+1}S \\ d^0 M \leq n \end{cases}.$$

$$d^0 M \leq n \Rightarrow \exists \alpha_0, \dots, \alpha_{n-1}, \alpha_n \in K \text{ tq : } M = \sum_{k=0}^n \alpha_k X^k.$$

$$\text{Posons } M_0 = \sum_{k=0}^{n-1} \alpha_k X^k \text{ alors on a : } \begin{cases} M = \sum_{k=0}^n \alpha_k X^k = \sum_{k=0}^{n-1} \alpha_k X^k + \alpha_n X^n = M_0 + \alpha_n X^n \\ d^0 M_0 \leq n-1 \end{cases} .$$

$$\text{Par suite on a : } A = B(M_0 + \alpha_n X^n) + X^{n+1}S = BM_0 + \alpha_n BX^n + X^{n+1}S \\ = BM_0 + X^n(\alpha_n B + XS) \text{ et } d^0 M_0 \leq n-1.$$

D'après l'hypothèse de récurrence on a : $M_0 = Q_0$ et $\alpha_n B + XS = A_0$.

$$A_0 = \alpha_n B + XS \Rightarrow [\alpha_n = \alpha \text{ et } S = R].$$

$$\text{Donc : } \begin{cases} M = M_0 + \alpha_n X^n = Q_0 + \alpha X^n = Q \\ S = R \end{cases} .$$

D'où l'unicité.

Corollaire 3-7-3 :

Soient A et B deux polynômes à coefficients dans K .

Si $B(0)$ est non nul et si K est un corps commutatif alors pour tout entier naturel n le quotient et le reste de la division suivant les puissances croissantes de A par B à l'ordre n existent.

En effet :

Supposons que $B(0)$ est non nul et que K est un corps commutatif.

Alors le coefficient constant $B(0)$ de B est inversible, et par suite (d'après le théorème et définition 3-7-2) le quotient et le reste de la division suivant les puissances croissantes de A par B à l'ordre n existent.

Exemple 3-7-4 :

Dans $K = \mathbb{R}$, Soient $A = 7X - 18$, $B = 3X^2 - X + 2$ et $n = 3$

$\begin{aligned} A &= -18 + 7X \\ &\quad \underline{18 - 9X + 27X^2} \\ &\quad -2X + 27X^2 \\ &\quad \quad \underline{2X - X^2 + 3X^3} \\ &\quad \quad 26X^2 + 3X^3 \\ &\quad \quad \underline{-26X^2 + 13X^3 - 39X^4} \\ &\quad \quad \quad 16X^3 - 39X^4 \\ &\quad \quad \quad \underline{-16X^3 + 8X^4 - 24X^5} \\ &\quad \quad \quad -31X^4 - 24X^5 \\ &= -X^4(24X + 31) \end{aligned}$	$\begin{aligned} B &= 2 - X + 3X^2 \\ Q &= -9 - X + 13X^2 + 8X^3 \end{aligned}$
---	---

Donc : $8X^3 + 13X^2 - X - 9$ est le quotient de la division suivant les puissances croissantes de A par B à l'ordre 3.

$-X^4(24X + 31)$ est le reste de la division suivant les puissances croissantes de A par B à l'ordre 3.

4-Arithmétique des polynômes :

Dans tout le paragraphe K étant un corps commutatif.

4-1- $p.g.c.d$ de deux polynômes :

Définition 4-1-1 :

Soient A, B et C des polynômes à coefficients dans K .

On dit que D est un $p.g.c.d$ de A et B si on a les deux propriétés suivantes :

i) D est un diviseur commun de A et B . C'est à dire :
$$\begin{cases} D|A \\ D|B \end{cases}.$$

ii) Tous les diviseurs communs de A et B sont des diviseurs de D .

C'est à dire $\forall \Delta \in K[X] : \begin{cases} \Delta|A \\ \Delta|B \end{cases} \Rightarrow \Delta|D$

Propriétés 4-1-2 :

Soient A et B deux polynômes à coefficients dans K .

1) Pour qu'un polynôme $D \in K[X]$ soit un $p.g.c.d$ de A et B il faut et il suffit que :

$$A \cdot K[X] + B \cdot K[X] = D \cdot K[X].$$

2) A et B possèdent au moins un $p.g.c.d$.

3) Si D est un $p.g.c.d$ de A et B alors les $p.g.c.d$ de A et B sont les associés de D .

C'est à dire si D est un $p.g.c.d$ de A et B alors pour tout polynôme $\Delta \in K[X]$,
[Δ est un $p.g.c.d$ de A et B] $\Leftrightarrow \Delta \sim D$

4) Si D est un $p.g.c.d$ de A et B alors il existe $U, V \in K[X]$ tels que : $UA + VB = D$.

5) Si $d^0 B \geq 1$ et si D est un $p.g.c.d$ de A et B alors il existe $U, V \in K[X]$ tels que :

$$\begin{cases} UA + VB = D \\ d^0 U < d^0 B \end{cases}.$$

Si de plus $d^0 A \geq 1$ on a aussi $d^0 V < d^0 A$.

6) Si $K = \mathbb{C}$ et si D est un $p.g.c.d$ de A et B alors $\overline{D}$ est un $p.g.c.d$ de $\overline{A}$ et $\overline{B}$.

7) A est un $p.g.c.d$ de A et B si et seulement si $A|B$.

8) A est un $p.g.c.d$ de A et 0 .

9) 0 est un $p.g.c.d$ de A et B si et seulement si $A = B = 0$.

10) 0 est le seul $p.g.c.d$ de 0 et 0 .

11) $\forall \alpha \in K^* : \alpha$ est un $p.g.c.d$ de A et α .

12) $\forall \alpha \in K^* : 1$ est un $p.g.c.d$ de A et α .

13) Si $B \neq 0$ et si R est le reste de la division euclidienne de A par B alors les $p.g.c.d$ de A et B sont les $p.g.c.d$ de B et R .

Démonstration :

1) Soit D un polynôme à coefficients dans K .

$\Rightarrow$) Si D est un $p.g.c.d$ de A et B :

★ Puisque D est un $p.g.c.d$ de A et B alors D est un diviseur commun de A et B ,
donc (d'après la propriété 3-4-2-5)-a)) $A \cdot K[X] + B \cdot K[X] \subset D \cdot K[X]$.

★ Puisque K est un corps commutatif alors (d'après le théorème 3-5-3), $K[X]$ est un anneau principal, et par suite $A \cdot K[X] + B \cdot K[X]$ est un idéal principal de $K[X]$. Donc il existe $\Delta \in K[X]$ tel que : $A \cdot K[X] + B \cdot K[X] = \Delta \cdot K[X]$.
Alors (d'après la propriété 3-4-2-5-a)), Δ est un diviseur commun de A et B .
Donc Δ est un diviseur de D (car D est un p.g.c.d de A et B).
Par conséquent : $D \cdot K[X] \subset \Delta \cdot K[X] = A \cdot K[X] + B \cdot K[X]$.

Ce qui montre que $A \cdot K[X] + B \cdot K[X] = D \cdot K[X]$.

$\Leftrightarrow$) Si on a : $A \cdot K[X] + B \cdot K[X] = D \cdot K[X]$:

★ Puisque $A \cdot K[X] + B \cdot K[X] = D \cdot K[X] \subset D \cdot K[X]$, alors (d'après la propriété 3-4-2-5-a)) D est un diviseur commun de A et B .

★ Soit Δ un diviseur commun quelconque de A et B .

D'après la propriété 3-4-2-5-a), $A \cdot K[X] + B \cdot K[X] \subset \Delta \cdot K[X]$.

Par suite on a : $D \cdot K[X] = A \cdot K[X] + B \cdot K[X] \subset \Delta \cdot K[X] \Rightarrow \Delta | D$.

Donc D est un p.g.c.d de A et B .

Ce qui montre que D est un p.g.c.d de A et B si seulement si

$A \cdot K[X] + B \cdot K[X] = D \cdot K[X]$.

2) Puisque $A \cdot K[X] + B \cdot K[X]$ est un idéal principal de $K[X]$ alors il existe un polynôme $D \in K[X]$ tel que : $A \cdot K[X] + B \cdot K[X] = D \cdot K[X]$.

Donc D est un p.g.c.d de A et B .

3) Soit D est un p.g.c.d de A et B , et soit Δ un polynôme quelconque à coefficients dans K

Puisque D est un p.g.c.d de A et B alors (d'après 1)) on a :

$$A \cdot K[X] + B \cdot K[X] = D \cdot K[X].$$

$$[\Delta \text{ est un p.g.c.d de } A \text{ et } B] \Leftrightarrow A \cdot K[X] + B \cdot K[X] = \Delta \cdot K[X] \text{ (d'après 1))}$$

$$\Leftrightarrow \Delta \cdot K[X] = D \cdot K[X]$$

$$\Leftrightarrow \Delta \sim D.$$

Donc les p.g.c.d de A et B sont les associés de D .

4) Soit D est un p.g.c.d de A et B .

D'après 1) on a : $A \cdot K[X] + B \cdot K[X] = D \cdot K[X]$. Alors $D \in A \cdot K[X] + B \cdot K[X]$.

Donc il existe $U, V \in K[X]$ tels que : $UA + VB = D$.

5) Supposons que $d^0 B \geq 1$ et que D est un p.g.c.d de A et B .

Alors il existe $M, N \in K[X]$ tels que : $MA + NB = D$.

Soient Q le quotient de la division euclidienne de M par B et U le reste de la division

$$\text{euclidienne de } M \text{ par } B \text{ On a alors : } \begin{cases} M = QB + U \\ d^0 U < d^0 B \end{cases}.$$

Par suite on a : $(U + QB)A + NB = D \Rightarrow UA + QBA + NB = D \Rightarrow UA + (QA + N)B = D$.

$$\text{En posant } V = QA + N, \text{ on obtient donc : } \begin{cases} UA + VB = D \\ d^0 U < d^0 B \end{cases}.$$

Dans ce cas supposons que $d^0 A \geq 1$.

Puisque D est un diviseur de A et puisque A est non nul alors :

$$d^0 D \leq d^0 A < d^0 A + 1 \leq d^0 A + d^0 B.$$

$$UA + VB = D \Rightarrow VB = D - UA$$

$$\Rightarrow d^0 V + d^0 B = d^0 (VB) = d^0 (D - UA) \leq \max(d^0 D, d^0 (UA)).$$

$$\begin{cases} d^0 D < d^0 A + d^0 B \\ d^0 (UA) = d^0 U + d^0 A < d^0 A + d^0 B \end{cases} \Rightarrow \max(d^0 D, d^0 (UA)) < d^0 A + d^0 B.$$

Par suite on a : $d^0 V + d^0 B < d^0 A + d^0 B \Rightarrow d^0 V < d^0 A$.

- 6) Supposons que $K = \mathbb{C}$ et soit D un p.g.c.d de A et B .
- ★ Puisque D est un diviseur commun de A et B alors (d'après la propriété 3-4-2-1)) $\overline{D}$ est aussi un diviseur commun de $\overline{A}$ et $\overline{B}$.
 - ★ Soit Δ un diviseur commun quelconque de $\overline{A}$ et $\overline{B}$.
Alors (d'après la propriété 3-4-2-1)) $\overline{\Delta}$ est un diviseur commun de $\overline{\overline{A}} = A$ et $\overline{\overline{B}} = B$.
Par suite $\overline{\Delta}$ est un diviseur de D (car D est un p.g.c.d de A et B).
D'après la propriété 3-4-2-1)) on a donc $\Delta = \overline{\overline{\Delta}}$ est un diviseur de $\overline{D}$.
Ce qui montre que $\overline{D}$ est un p.g.c.d de $\overline{A}$ et $\overline{B}$.
- 7) $[A \text{ est un p.g.c.d de } A \text{ et } B] \Leftrightarrow A \cdot K[X] + B \cdot K[X] = A \cdot K[X] \Leftrightarrow B \cdot K[X] \subset A \cdot K[X] \Leftrightarrow A|B$.
- 8) Puisque A est un diviseur de 0 alors (d'après 7)) A est un p.g.c.d de A et 0.
- 9) $\Rightarrow$) **Si 0 est un p.g.c.d de A et B :**
Alors 0 est un diviseur commun de A et B . Donc $A = B = 0$.
 $\Leftarrow$) **Si $A = B = 0$:**
On a : $A \cdot K[X] + B \cdot K[X] = 0 \cdot K[X] + 0 \cdot K[X] = \{0\} + 0 \cdot K[X] = 0 \cdot K[X]$.
Donc 0 est un p.g.c.d de A et B .
Ce qui montre que 0 est un p.g.c.d de A et B si seulement si $A = B = 0$.
- 10) D'après 9), 0 est un p.g.c.d de 0 et 0.
Puisque 0 est le seul associé 0 alors 0 est le seul p.g.c.d de 0 et 0.
- 11) $\forall \alpha \in K^* : \alpha$ est un diviseur de A , donc d'après 7) α est un p.g.c.d de A et α .
- 12) $\forall \alpha \in K^* : \begin{cases} \alpha \text{ est un p.g.c.d de } A \text{ et } \alpha \text{ (d'après 7))} \\ \alpha \text{ est associé à } 1 \end{cases} \Rightarrow 1 \text{ est un p.g.c.d de } A \text{ et } \alpha$.
- 13) Supposons que $B \neq 0$ et que R est le reste de la division euclidienne de A par B et D un polynôme quelconque à coefficients dans K .
 $\Rightarrow$) **Si D est un p.g.c.d de A et B :**
★ Puisque D est un diviseur commun de A et B alors (d'après la propriété 3-4-2-6)) D est aussi un diviseur commun de B et R .
★ Soit Δ un diviseur commun quelconque de B et R .
D'après la propriété 3-4-2-6), Δ est aussi un diviseur commun de A et B .
Donc Δ un diviseur de D (car D est un p.g.c.d de A et B).
Ce qui prouve que D est un p.g.c.d de A et R .
 $\Rightarrow$) **Si D est un p.g.c.d de B et R :**
★ Puisque D est un diviseur commun de B et R alors (d'après la propriété 3-4-2-6)) D est aussi un diviseur commun de A et B .
★ Soit Δ un diviseur commun quelconque de A et B .
D'après la propriété 3-4-2-6), Δ est aussi un diviseur commun de B et R .
Donc Δ un diviseur de D (car D est un p.g.c.d de B et R).
Ce qui prouve que D est un p.g.c.d de A et B .
On a alors montrer que les p.g.c.d de A et B sont les p.g.c.d de B et R .

Définition 4-1-3 :

Soient $R_0, R_1, \dots, R_n$ des polynômes à coefficients dans K .

On dit que $(R_0, R_1, \dots, R_n)$ est une suite euclidienne si on a les 4 propriétés suivantes :

- i) $n \geq 2$
- ii) $\forall k = 0, 1, \dots, n : R_k \neq 0$
- iii) $\forall k = 2, \dots, n : R_k$ est le reste de la division euclidienne de R_{k-2} par R_{k-1}
- iv) $R_n | R_{n-1}$ c'est à dire que le reste de la division euclidienne de R_{n-1} par R_n est nul.

L'entier n est appelé la longueur de la suite $(R_0, R_1, \dots, R_n)$.

Définition 4-1-4 :

Soient A et B deux polynômes à coefficients dans K et $(R_0, R_1, \dots, R_n)$ une suite euclidienne. Si $R_0 = A$ et si $R_1 = B$ on dit que $(R_0, R_1, \dots, R_n)$ est une suite euclidienne de (A, B) .

Remarque 4-1-5 :

Soient A et B deux polynômes à coefficients dans K .

Si (A, B) possède une suite euclidienne alors: $A \neq 0$, $d^0 B \geq 1$ et B n'est pas un diviseur de A .

En effet :

Supposons que (A, B) possède une suite euclidienne $(R_0, R_1, \dots, R_n)$.

★ $A = R_0 \neq 0$.

★ Puisque le reste R_2 de la division euclidienne de $R_0 = A$ par $R_1 = B$ n'est pas nul alors B n'est pas un diviseur de A .

Lemme 4-1-6 :

Soient A et B deux polynômes non nul à coefficients dans K et R le reste de la division euclidienne de A par B .

Si $R \neq 0$ et si R divise B alors (A, B, R) est une suite euclidienne de (A, B) et c'est la seule suite euclidienne de (A, B) .

Démonstration :

★ Posons $R_0 = A$, $R_1 = B$ et $R_2 = R$. On a alors :

$R_0 = A$, $R_1 = B$, $R_2 = R$ est le reste de la division euclidienne de $R_0 = A$ par $R_1 = B$ et $R_2 = R$ est un diviseur de R_1 . C'est à dire :

$R_0 = A$, $R_1 = B$, $\forall i = 2, \dots, n : R_i$ est le reste de la division euclidienne de R_{i-2} par R_{i-1} et $R_2 | R_1$.

Alors $(A, B, R) = (R_0, R_1, R_2)$ est une suite euclidienne de (A, B) .

★ Soit $(S_0, S_1, \dots, S_n)$ une suite euclidienne quelconque de (A, B) . On a :

$S_0 = A = R_0$ et $S_1 = B = R_1$.

Puisque S_2 est le reste de la division euclidienne de $S_0 = R_0$ par $S_1 = R_1$ alors $S_2 = R_2$.

Supposons que $n \geq 3$.

$$\begin{cases} S_2 = R_2 = R \in K^* \\ S_3 \text{ est le reste de la division euclidienne de } S_1 \text{ par } S_2 \end{cases} \Rightarrow S_3 = 0.$$

Ce qui est absurde. Donc $n = 2$, par suite on a :

$(S_0, S_1, \dots, S_n) = (S_0, S_1, S_3) = (R_0, R_1, R_2)$ D'où l'unicité.

Théorème et définition 4-1-7 (Algorithme d'Euclide) :

Tout couple (A, B) de polynômes non nuls à coefficients dans K tel que B ne soit pas un diviseur de A , admet une suite euclidienne et une seule.

Pratiquement pour déterminer la suite euclidienne de A et B on effectue les divisions suivantes :

$$\begin{array}{c|c|c|c|c|c|c|c|c|c} R_0 = A & R_1 = B & R_1 = B & R_2 & \dots & R_{n-2} & R_{n-1} & R_n & R_{n-1} & R_n \\ R_2 & Q_0 & R_3 & Q_1 & & R_n & Q_{n-2} & 0 & Q_{n-1} \end{array}$$

R_n est le dernier reste non nul.

La recherche de la suite euclidienne de (A, B) est appelée l'Algorithme d'Euclide appliquée (A, B) . suite euclidienne et une seule.

Démonstration :

- ★ Pour tout couple (A, B) de polynômes non nul à coefficients dans K tel que B ne soit pas un diviseur de A , on a : $d^0 B \geq 1$.
- ★ Montrons par récurrence que pour tout entier naturel non nul k , si (A, B) est un couple de polynômes non nuls à coefficients dans K tel que B ne soit pas un diviseur de A et tel que $d^0 B = k$ alors (A, B) admet suite euclidienne et une seule.

- Pour $k = 1$:

Soit (A, B) un couple de polynômes non nul à coefficients dans K tel que B ne soit pas un diviseur de A et tel que $d^0 B = k = 1$.

Soit R le reste de la division euclidienne de A par B .

$d^0 R < d^0 B = k = 1 \Rightarrow d^0 R \leq 0 \Rightarrow R \in K \Rightarrow R \in K^*$ (car B ne divise pas A).

$R \in K^* \Rightarrow R|B$.

Donc (d'après le lemme 4-1-6) (A, B, R) est une suite euclidienne de (A, B) et c'est la seule suite euclidienne de (A, B) .

- Pour $k - 1$:

Supposons que si (A, B) est un couple de polynômes non nuls à coefficients dans K tel que B ne soit pas un diviseur de A et tel que $d^0 B \leq k - 1$ alors (A, B) admet suite euclidienne et une seule.

- Pour k :

Montrons qu'alors si (A, B) est un couple de polynômes non nuls à coefficients dans K tel que B ne soit pas un diviseur de A et tel que $d^0 B \leq k$ alors (A, B) admet suite euclidienne et une seule.

Soit (A, B) un couple de polynômes non nuls à coefficients dans K tel que B ne soit pas un diviseur de A et tel que $d^0 B = k$.

Soit R le reste de la division euclidienne de A par B .

R n'est pas nul (car B n'est pas un diviseur de A) et $d^0 R \leq k - 1$ (car $d^0 R < d^0 B$).

• Si R est un diviseur de B :

Alors (d'après le lemme 4-1-6) (A, B, R) est une suite euclidienne de (A, B) et c'est la seule suite euclidienne de (A, B) .

• Si R n'est pas un diviseur de B :**• Existence :**

Puisque B et R sont non nuls, R n'est pas un diviseur de B et $d^0 R \leq k - 1$ alors, d'après l'hypothèse de récurrence, (B, R) admet une suite euclidienne $(P_0, P_1, \dots, P_n)$ et une seule.

Posons : $R_0 = A$ et $\forall i = 1, \dots, n+1 : R_i = P_{i-1}$. On a alors :

$R_0 = A, R_1 = P_0 = B, R_2 = P_1 = R$ est le reste de la division euclidienne de $A = R_0$ par $B = R_1, \forall i = 3, \dots, n+1 : R_i = P_{i-1}$ est le reste de la division euclidienne de $P_{i-3} = R_{i-2}$ par $P_{i-2} = R_{i-1}$ et $R_{n+1} = P_n$ est un diviseur de $P_{n-1} = R_n$.

Donc $(R_0, R_1, \dots, R_n, R_{n+1})$ est une suite euclidienne de (A, B) .

D'où l'existence.

• **Unicité :**

Soit $(S_0, S_1, \dots, S_m)$ une suite euclidienne quelconque de (A, B)

Puisque S_2 est le reste de la division euclidienne de $S_0 = A$ par $S_1 = B$ alors $S_2 = R$

Aors $S_2 = R$ ne divise pas S_1 , par suite $m \neq 2$ et donc $m \geq 3$.

$\forall i = 0, 1, \dots, m-1$: posons $Q_i = S_{i+1}$. On a alors :

$Q_0 = S_1 = B, Q_1 = S_2 = R, \forall i = 2, \dots, m-1 : Q_i = S_{i+1}$ est le reste de la division euclidienne de $Q_{i-2} = S_{i-1}$ par $Q_{i-1} = S_i$ et $Q_{m-1} = S_m$ divise $Q_{m-2} = S_{m-1}$

Donc $(Q_0, Q_1, \dots, Q_{m-1})$ est une suite euclidienne de (B, R) .

On a vu que :
$$\left\{ \begin{array}{l} B \text{ et } R \text{ ne sont pas nuls} \\ R \text{ n'est pas un diviseur de } B \\ d^0 R \leq k-1 \text{ (car } d^0 R < d^0 B) \end{array} \right.$$

Ce qui prouve, d'après l'hypothèse de récurrence que (B, R) admet une suite euclidienne et une seule. Par suite on a : $(Q_0, Q_1, \dots, Q_{m-1}) = (P_0, P_1, \dots, P_n)$.

Alors : $m-1 = n$ et $\forall i = 0, 1, \dots, n : S_i = P_i$.

Par conséquent on a :
$$\left\{ \begin{array}{l} m = n+1 \\ S_0 = A = R_0 \\ \forall i = 1, \dots, n : S_i = Q_{i-1} = P_{i-1} = R_i \end{array} \right.$$

Donc : $(S_0, S_1, \dots, S_m) = (R_0, R_1, \dots, R_{n+1})$.

D'où l'unicité.

Théorème et définition 4-1-8 (Algorithme d'Euclide) :

Soit (A, B) un couple de polynômes non nuls à coefficients dans K .

Si B ne divise pas A et si $(R_0, R_1, \dots, R_n)$ est la suite euclidienne de (A, B) alors R_n est un $p.g.c.d$ de A et B .

Démonstration :

Montrons par récurrence sur $n \geq 2$ que pour tout couple (A, B) de polynômes non nuls à coefficients dans K , si B ne divise pas A et si $(R_0, R_1, \dots, R_n)$ est la suite euclidienne de (A, B) de longueur n alors R_n est un $p.g.c.d$ de A et B .

- **Pour $n = 2$:**

Soit (A, B) un couple de polynômes non nuls à coefficients dans K tel que B ne soit pas un diviseur A et tel que (R_0, R_1, R_2) soit la suite euclidienne de (A, B) de longueur 2.

R_2 est un $p.g.c.d$ de R_1 et R_2 (car R_2 est un diviseur de R_1).

Puisque R_2 est un $p.g.c.d$ de R_1 et R_2 et puisque R_2 est le reste de la division euclidienne de $R_0 = A$ par $R_1 = B$ alors R_2 est un $p.g.c.d$ de $R_0 = A$ et $R_1 = B$.

Donc $R_n = R_2$ est un $p.g.c.d$ de A et B .

- **Pour $n - 1$:**

Supposons que si (A, B) est un couple de polynômes non nuls à coefficients dans K tel que B ne soit pas un diviseur A et que $(R_0, R_1, \dots, R_{n-1})$ est la suite euclidienne de (A, B) de longueur $n - 1$ alors R_{n-1} est un $p.g.c.d$ de A et B .

- **Pour n :**

Montrons qu'alors si (A, B) est un couple de polynômes non nuls à coefficients dans K tel que B ne soit pas un diviseur A et tel que $(R_0, R_1, \dots, R_n)$ soit la suite euclidienne de (A, B) de longueur n alors R_n est un $p.g.c.d$ de A et B .

Soit (A, B) un couple de polynômes non nuls à coefficients dans K tel que B ne soit pas un diviseur A et tel que $(R_0, R_1, \dots, R_n)$ soit la suite euclidienne de (A, B) de longueur n .

Posons : $C = R_2$ et $\forall i = 0, 1, \dots, n - 1 : S_i = R_{i+1}$. On a alors :

$$\star S_0 = R_1 \quad \text{et} \quad S_1 = R_2 = C.$$

$$\star \forall i = 2, \dots, n - 1 : S_i = R_{i+1} \text{ est le reste de la division euclidienne de } S_{i-2} = R_{i-1} \text{ par } S_{i-1} = R_i.$$

$$\star S_{n-1} = R_n \text{ est un diviseur de } S_{n-2} = R_{n-1}.$$

Par suite $(S_0, S_1, \dots, S_{n-1})$ est la suite euclidienne de (B, C) de longueur $n - 1$.

Ce qui prouve, d'après l'hypothèse de récurrence que $S_{n-1} = R_n$ est un $p.g.c.d$ de B et C .

Puisque R_n est un $p.g.c.d$ de B et C , et puisque $C = R_2$ est le reste de la division euclidienne de $R_0 = A$ par $R_1 = B$ alors (d'après la propriété 3-4-2-6)) R_n est un $p.g.c.d$ de A et B .

Exemple 4-1-8 :

Dans $\mathbb{R}[X]$, Soient $A = 8X^5 + 4X^4 + 10X^3 - 5X^2 + X - 1$ et $B = 4X^4 + 4X^3 + 5X^2 - 2X - 1$

$$\begin{array}{l} R_0 = A = 8X^5 + 4X^4 + 10X^3 - 5X^2 + X - 1 \\ R_2 = 4X^3 + 4X^2 + X - 2 \end{array} \left| \begin{array}{l} R_1 = B = 4X^4 + 4X^3 + 5X^2 - 2X - 1 \\ Q_0 = 2X - 1 \end{array} \right.$$

$$\begin{array}{l} R_1 = B = 4X^4 + 4X^3 + 5X^2 - 2X - 1 \\ R_3 = 4X^2 - 1 \end{array} \left| \begin{array}{l} R_2 = 4X^3 + 4X^2 + X - 2 \\ Q_1 = X \end{array} \right.$$

$$\begin{array}{l} R_2 = 4X^3 + 4X^2 + X - 2 \\ R_4 = 2X - 1 \end{array} \left| \begin{array}{l} R_3 = 4X^2 - 1 \\ Q_2 = X + 1 \end{array} \right.$$

$$\begin{array}{l} R_3 = 4X^2 - 1 \\ 0 \end{array} \left| \begin{array}{l} R_4 = 2X - 1 \\ Q_3 = 2X + 1 \end{array} \right.$$

Donc (R_0, R_1, R_3, R_4) est la suite euclidienne de A et B telle que :

$$\left\{ \begin{array}{l} R_0 = A = 8X^5 + 4X^4 + 10X^3 - 5X^2 + X - 1 \\ R_1 = B = 4X^4 + 4X^3 + 5X^2 - 2X - 1 \\ R_2 = 4X^3 + 4X^2 + X - 2 \\ R_3 = 4X^2 - 1 \\ R_4 = 2X - 1 \end{array} \right.$$

Alors $R_4 = 2X - 1$ est un $p.g.c.d$ de A et B .

Théorème et définition 4-1-9 (Algorithme d'Euclide):

Soient A et B deux polynômes non nuls à coefficients dans K .

Si B ne divise pas A , $(R_0, R_1, \dots, R_n)$ est la suite euclidienne de (A, B)

et si $Q_0, Q_1, \dots, Q_{n-2}$ sont les quotients des divisions euclidiennes

respectivement des polynômes $R_0, R_1, \dots, R_{n-2}$ par $R_1, R_2, \dots, R_{n-1}$

alors il existe d'une façon unique des polynômes :

$U = U_0, U_1, \dots, U_{n-2}, V = V_0, V_1, \dots, V_{n-2}$ qui vérifient les 4 propriétés suivantes :

i) $U_{n-2} = 1$

ii) $V_{n-2} = -Q_{n-2}$

iii) $\forall k = 0, 1, \dots, n-2 : U_k R_k + V_k R_{k+1} = R_n$

iv) Si $n \geq 3$ alors : $\forall k = 0, 1, \dots, n-3 : \begin{cases} U_k = V_{k+1} \\ V_k = U_{k+1} - V_{k+1} Q_k \end{cases}$

On a aussi la propriété suivante : $\forall k = 0, 1, \dots, n-2 : \begin{cases} d^0 U_k < d^0 R_{k+1} \\ d^0 V_k < d^0 R_k \end{cases}$

En particulier on a la propriété suivante : $\begin{cases} UA + VB = R_n \\ d^0 U < d^0 B \\ d^0 V < d^0 A \end{cases}$

La recherche des deux polynômes U et V est appelée "la recherche des deux polynômes $U, V \in K[X]$ tels que : $UA + V = R_n$ en utilisant l'Algorithme d'Euclide".

Pratiquement pour chercher les des deux polynômes U et V :

On effectue les divisions suivantes :

$$\begin{array}{c|c} R_0 = A & R_1 = B \\ \hline R_2 & Q_0 \end{array} \quad \begin{array}{c|c} R_1 = B & R_2 \\ \hline R_3 & Q_1 \end{array} \quad \dots \quad \begin{array}{c|c} R_{n-2} & R_{n-1} \\ \hline R_n & Q_{n-2} \end{array} \quad \begin{array}{c|c} R_{n-1} & R_n \\ \hline 0 & Q_{n-1} \end{array}$$

On a donc : $\begin{cases} A = Q_0 B + R_2 \\ B = Q_1 R_2 + R_3 \\ \dots \\ R_{n-3} = Q_{n-3} R_{n-2} + R_{n-1} \\ R_{n-2} = Q_{n-2} R_{n-1} + R_n \end{cases} \Leftrightarrow \begin{cases} A - Q_0 B = R_2 \\ B - Q_1 R_2 = R_3 \\ \dots \\ R_{n-3} - Q_{n-3} R_{n-2} = R_{n-1} \\ R_{n-2} - Q_{n-2} R_{n-1} = R_n \end{cases}$

On pose $U_{n-2} = 1$ et $V_{n-2} = -Q_{n-2}$. On a donc : $U_{n-2} R_{n-2} + V_{n-2} R_{n-1} = R_n$

Puis on remplace dans cette équation le polynôme R_{n-1} par sa valeur $R_{n-3} - Q_{n-3} R_{n-2}$

On obtient : $U_{n-2} R_{n-2} + V_{n-2} R_{n-1} = R_n \Leftrightarrow U_{n-2} R_{n-2} + V_{n-2} (R_{n-3} - Q_{n-3} R_{n-2}) = R_n$
 $\Leftrightarrow U_{n-2} R_{n-2} + V_{n-2} R_{n-3} - V_{n-2} Q_{n-3} R_{n-2} = R_n$
 $\Leftrightarrow V_{n-2} R_{n-3} + U_{n-2} R_{n-2} - V_{n-2} Q_{n-3} R_{n-2} = R_n$
 $\Leftrightarrow V_{n-2} R_{n-3} + (U_{n-2} - V_{n-2} Q_{n-3}) R_{n-2} = R_n$.

On pose : $U_{n-3} = V_{n-2}$ et $V_{n-3} = U_{n-2} - V_{n-2} Q_{n-3}$.

Si $n = 3$ alors : $U = U_0 = V_1$ et $V = V_0 = U_1 - V_1 Q_0$.

Si $n \geq 4$ on remplace dans l'équation $U_{n-3} R_{n-3} + V_{n-3} R_{n-2} = R_n$ le polynôme R_{n-2} par sa valeur $R_{n-4} - Q_{n-4} R_{n-3}$. On obtient :

$U_{n-3} R_{n-3} + V_{n-3} R_{n-2} = R_n \Leftrightarrow U_{n-3} R_{n-3} + V_{n-3} (R_{n-4} - Q_{n-4} R_{n-3}) = R_n$
 $\Leftrightarrow U_{n-3} R_{n-3} + V_{n-3} R_{n-4} - V_{n-3} Q_{n-4} R_{n-3} = R_n$
 $\Leftrightarrow V_{n-3} R_{n-4} + U_{n-3} R_{n-3} - V_{n-3} Q_{n-4} R_{n-3} = R_n$
 $\Leftrightarrow V_{n-3} R_{n-4} + (U_{n-3} - V_{n-3} Q_{n-4}) R_{n-3} = R_n$

On pose : $U_{n-4} = V_{n-3}$ et $V_{n-4} = U_{n-3} - V_{n-3}Q_{n-4}$.

Et ainsi de suite jusqu'à ce qu'on trouve les polynômes $U = U_0$ et $V = V_0$.

Exemple 4-1-10 :

Dans $\mathbb{R}[X]$ soient $A = 8X^5 + 4X^4 + 10X^3 - 5X^2 + X - 1$ et $B = 4X^4 + 4X^3 + 5X^2 - 2X - 1$.

Donc (R_0, R_1, R_3, R_4) est la suite euclidienne de (A, B) telle que :

$$\begin{cases} R_0 = A = 8X^5 + 4X^4 + 10X^3 - 5X^2 + X - 1 \\ R_1 = B = 4X^4 + 4X^3 + 5X^2 - 2X - 1 \\ R_2 = 4X^3 + 4X^2 + X - 2 \\ R_3 = 4X^2 - 1 \\ R_4 = 2X - 1 \end{cases}$$

On a vu aussi d'après les divisions euclidiennes que :

$Q_0 = 2X - 1$, $Q_1 = X$ et $Q_2 = X + 1$. On a alors :

$$\begin{cases} A = (2X - 1)B + 4X^3 + 4X^2 + X - 2 \\ B = X(4X^3 + 4X^2 + X - 2) + 4X^2 - 1 \\ 4X^3 + 4X^2 + X - 2 = (X + 1)(4X^2 - 1) + 2X - 1 \end{cases}$$

$$\Leftrightarrow \begin{cases} A - (2X - 1)B = 4X^3 + 4X^2 + X - 2 \\ B - X(4X^3 + 4X^2 + X - 2) = 4X^2 - 1 \\ 4X^3 + 4X^2 + X - 2 - (X + 1)(4X^2 - 1) = 2X - 1 \end{cases}$$

On a alors :

$$4X^3 + 4X^2 + X - 2 - (X + 1)[B - X(4X^3 + 4X^2 + X - 2)] = 2X - 1$$

$$4X^3 + 4X^2 + X - 2 - (X + 1)B + (X^2 + X)(4X^3 + 4X^2 + X - 2) = 2X - 1$$

$$(X^2 + X + 1)(4X^3 + 4X^2 + X - 2) - (X + 1)B = 2X - 1$$

$$(X^2 + X + 1)[A - (2X - 1)B] - (X + 1)B = 2X - 1$$

$$(X^2 + X + 1)A - (2X^3 + X^2 + X - 1)B = 2X - 1$$

$$(X^2 + X + 1)A - (2X^3 + X^2 + 2X)B = 2X - 1 = R_4.$$

Alors : $U = X^2 + X + 1$ et $V = -(2X^3 + X^2 + 2X)$

$$\text{On a donc : } \begin{cases} UA + VB = 2X - 1 = R_4 \\ d^0 U = 2 \prec 4 = d^0 B \\ d^0 V = 3 \prec 5 = d^0 A \end{cases}.$$

Proposition et définition 4-1-11 :

Soient A et B deux polynômes à coefficients dans K et D un $p.g.c.d$ quelconque de A et B .

- **Si $D \neq 0$ (c'est à dire si $A \neq 0$ ou $B \neq 0$) :**

Alors A et B possèdent un $p.g.c.d$ unitaire et un seul noté $A \wedge B$ appelé le $p.g.c.d$ de A et B .

Si α est le coefficient dominant de D alors : $A \wedge B = \frac{1}{\alpha}D$.

- **Si $D = 0$ (c'est à dire si $A = B = 0$) :**

Alors 0 est le seul $p.g.c.d$ de 0 et 0 appelé le $p.g.c.d$ de 0 et 0 et on note $0 \wedge 0 = 0$.

En effet :

- **Si $D \neq 0$ (c'est à dire si $A \neq 0$ ou $B \neq 0$) :**

Soit α le coefficient dominant de D .

Puisque $\frac{1}{\alpha}D$ est le seul polynôme unitaire de $K[X]$ associé à D alors $\frac{1}{\alpha}D$ est un $p.g.c.d$ unitaire de A et B , et c'est le seul $p.g.c.d$ unitaire de A et B .

- **Si $D = 0$ (c'est à dire si $A = B = 0$) :**

Puisque 0 est le seul polynôme de $K[X]$ associé à lui même alors 0 est le seul $p.g.c.d$ de 0 et 0.

Exemple 4-1-12 :

Dans $\mathbb{R}[X]$ soient $A = 8X^5 + 4X^4 + 10X^3 - 5X^2 + X - 1$ et $B = 4X^4 + 4X^3 + 5X^2 - 2X - 1$.

On a vu que $2X - 1$ est un $p.g.c.d$ de A et B . Donc : $A \wedge B = \frac{1}{2}(2X - 1) = X - \frac{1}{2}$.

Remarque 4-1-13 :

Si A et B sont des polynômes à coefficients complexes alors : $\overline{A \wedge B} = \overline{A} \wedge \overline{B}$.

En effet :

★ **Si $A \wedge B = 0$:**

Alors $A = B = 0$ et par suite on a :

$$\overline{A \wedge B} = \overline{0 \wedge 0} = \overline{0 \wedge 0} = \overline{0} = \overline{0 \wedge 0} = \overline{A \wedge B}.$$

★ **Si $A \wedge B \neq 0$:**

Alors

$$\begin{cases} A \wedge B \text{ est un } p.g.c.d \text{ de } A \text{ et } B \\ A \wedge B \text{ est unitaire} \end{cases} \Rightarrow \begin{cases} \overline{A \wedge B} \text{ est un } p.g.c.d \text{ de } A \text{ et } B \\ \overline{A \wedge B} \text{ est unitaire} \end{cases}$$

$$\Rightarrow \overline{A \wedge B} = \overline{A \wedge B}.$$

Définition 4-1-14 :

Soient A et B deux polynômes à coefficients dans K .

Si $A \wedge B = 1$ on dit que " A est premier à B " ou " A et B sont premiers entre eux".

Remarque 4-1-15 :

Soient A et B deux polynômes à coefficients dans K . Les propriétés suivantes sont équivalentes :

- i) A et B sont premiers entre eux.
- ii) 1 est un $p.g.c.d$ de A et B .
- iii) il existe un élément non nul α de K tel que α soit un $p.g.c.d$ de A et B .
- iv) les seuls diviseurs communs à A et B sont les constantes non nulles de K .

En effet :

★ **Si A et B sont premiers entre eux :**

Alors $A \wedge B = 1$ et par suite 1 est un $p.g.c.d$ de A et B . Donc "i) $\Rightarrow$ ii)" est vraie.

★ **Si 1 est un $p.g.c.d$ de A et B**

Il suffit de prendre $\alpha = 1$. Alors $\alpha = 1$ est un élément non nul de K et α est un $p.g.c.d$ de A et B .

Donc "ii) $\Rightarrow$ iii)" est vraie.

★ **Supposons qu'il existe un élément non nul α de K tel que α soit un p.g.c.d de A et B :**

Soit D un diviseur quelconque commun de A et B .

$$\begin{cases} D|A \\ D|B \end{cases} \Rightarrow D|\alpha \text{ (car } \alpha \text{ est un p.g.c.d de } A \text{ et } B) \Rightarrow \begin{cases} D \neq 0 \\ d^0 D \leq d^0 \alpha = 0 \end{cases} \Rightarrow d^0 D = 0.$$

Donc D est une constante non nulle de K .

On a prouvé que les seuls diviseurs communs à A et B sont les constantes non nulles de K .

Ce qui montre que "iii) $\Rightarrow$ iv)" est vraie.

★ **Supposons que les seuls diviseurs communs à A et B sont les constantes non nulles de K :**

$A \wedge B$ est un diviseur commun à A et B . Donc : $A \wedge B \in K^*$.

Puisque $A \wedge B \in K^*$ et puisque $A \wedge B$ est unitaire alors $A \wedge B = 1$.

Donc "iv) $\Rightarrow$ i)" est vraie.

Ce qui montre que les propriétés i) , ii) , iii) et iv) sont équivalentes.

4-2-Identité de Bezout et ses applications :

Théorème 4-2-1 (Identité de Bezout) :

Soient A et B deux polynômes à coefficients dans K .

Pour que A et B soient premiers entre eux il faut et il suffit qu'il existe deux polynômes

U et V à coefficients dans K tels que : $UA + VB = 1$.

C'est à dire : $A \wedge B = 1 \Leftrightarrow \exists U, V \in K[X] \text{ tq : } UA + VB = 1$.

En effet :

$$\begin{aligned} A \wedge B = 1 &\Leftrightarrow A \cdot K[X] + B \cdot K[X] = K[X] \Leftrightarrow 1 \in [A \cdot K[X] + B \cdot K[X]] \\ &\Leftrightarrow \exists U, V \in K[X] \text{ tq : } UA + VB = 1. \end{aligned}$$

Corollaire 4-2-2 :

Si $a, b \in K$ et si $a \neq b$ alors $X - a$ et $X - b$ sont premiers entre eux .

C'est à dire : $\forall a, b \in K : a \neq b \Rightarrow (X - a) \wedge (X - b) = 1$.

En effet :

$\forall a, b \in K \text{ tq : } a \neq b$: on a :

$(X - a) - (X - b) = X - a - X + b = b - a$. Par suite on a :

$$\begin{aligned} \frac{1}{b-a} [(X - a) - (X - b)] &= 1 \Rightarrow \frac{1}{b-a} (X - a) - \frac{1}{b-a} (X - b) = 1 \\ &\Rightarrow \frac{1}{b-a} (X - a) + \frac{1}{a-b} (X - b) = 1. \end{aligned}$$

Donc $X - a$ et $X - b$ sont premiers entre eux. C'est à dire : $(X - a) \wedge (X - b) = 1$.

Corollaire 4-2-3 :

Soient A, B et D des polynômes à coefficients dans K .

Pour que D soit un $p.g.c.d$ de A et B il faut et il suffit qu'il existe deux polynômes

$$A_0 \text{ et } B_0 \text{ à coefficients dans } K \text{ tels que : } \begin{cases} A = A_0 D \\ B = B_0 D \\ A_0 \wedge B_0 = 1 \end{cases} .$$

Si en particulier $D \neq 0$ (c'est à dire si $A \neq 0$ ou $B \neq 0$) les deux polynômes A_0, B_0 existent d'une façon unique et dans ce cas A_0 et B_0 sont les quotients de la division euclidienne des polynômes A et B par D .

Démonstration :

$\Rightarrow$) **Si D est un $p.g.c.d$ de A et B :**

- **Si $D = 0$:**

Alors $A = B = 0$. Il suffit de prendre $A_0 = B_0 = 1$ et on a :

$$\begin{cases} A = 0 = 1 \times 0 = A_0 D \\ B = 0 = 1 \times 0 = B_0 D \\ A_0 \wedge B_0 = 1 \wedge 1 = 1 \end{cases} .$$

- **Si $D \neq 0$:**

$$\begin{cases} D|A \\ D|B \end{cases} \Rightarrow \exists A_0, B_0 \in K[X] \quad tq : \begin{cases} A = A_0 D \\ B = B_0 D \end{cases} .$$

Puisque D est un $p.g.c.d$ de A et B alors il existe deux polynômes U et V à coefficients dans K tels que : $UA + VB = D$.

Par suite on a : $UA_0 D + VB_0 D = D \Rightarrow (UA_0 + VB_0)D = D \Rightarrow UA_0 + VB_0 = 1$.

D'après l'identité de Bezout, A_0 et B_0 sont premiers entre eux.

$$\text{On a donc : } \begin{cases} A = A_0 D \\ B = B_0 D \\ A_0 \wedge B_0 = 1 \end{cases} .$$

$\Leftarrow$) **S'il existe deux polynômes A_0 et B_0 à coefficients dans K premiers entre eux tels que $A = A_0 D$ et $B = B_0 D$:**

★ Puisque $A = A_0 D$ et $B = B_0 D$ alors D est un diviseur commun de A et B .

★ Soit Δ un diviseur commun quelconque de A et B .

Il existe alors deux polynômes P et Q dans $K[X]$ tels que : $A = P\Delta$ et $B = Q\Delta$.

$A_0 \wedge B_0 = 1 \Rightarrow \exists U, V \in K[X] \quad tq : UA_0 + VB_0 = 1$.

$$\begin{aligned} \text{On a donc : } (UA_0 + VB_0)D &= D \Rightarrow UA_0 D + VB_0 D = D \Rightarrow UA + VB = D \\ &\Rightarrow UP\Delta + VQ\Delta = D \Rightarrow (UP + VQ)\Delta = D \\ &\Rightarrow \Delta|D. \end{aligned}$$

Ce qui montre que D est un $p.g.c.d$ de A et B .

Dans ce cas :

$$\begin{cases} A = A_0 D \\ B = B_0 D \end{cases} \Rightarrow \begin{cases} A_0 \text{ est le quotient de la division euclidienne } A \text{ par } D \\ B_0 \text{ est le quotient de la division euclidienne } B \text{ par } D \end{cases} .$$

4-3-Identité de Gauss et ses applications :

Théorème 4-3-1 (Identité de Gauss) :

Soient A et B deux polynômes à coefficients dans K .

Si $A \neq 0$ alors A et B sont premiers entre eux si et seulement si on a propriété suivante :

$$\forall C \in K[X] : A|(BC) \Rightarrow A|C$$

C'est à dire : $\forall A, B \in K[X] : \text{si } A \neq 0 \text{ alors :}$

$$A \wedge B = 1 \Leftrightarrow [\forall C \in K[X] : A|(BC) \Rightarrow A|C].$$

Démonstration :

$\Rightarrow$) **Si A et B sont premiers entre eux :**

Soit C un polynôme à coefficients dans K tel que A soit un diviseur de BC .

Il existe alors un polynôme Q à coefficients dans K tel que $BC = AQ$.

Puisque A et B sont premiers entre eux, il existe deux polynômes U et V à coefficients dans K tels que : $UA + VB = 1$.

Par suite on a :

$$(UA + VB)C = C \Rightarrow UAC + VBC = C \Rightarrow UAC + VAQ = C \Rightarrow A(UC + VQ) = C.$$

Ce qui montre que A est un diviseur de C .

$\Leftarrow$) **Si on a : $\forall C \in K[X] : A|(BC) \Rightarrow A|C$:**

Soit D un diviseur commun de A et B .

Il existe alors il existe alors deux polynômes A_0 et B_0 à coefficients dans K tels que :

$$\begin{cases} A = A_0 D \\ B = B_0 D \end{cases} \text{ . Donc } A_0 \text{ est un diviseur de } A.$$

$$BA_0 = B_0 D A_0 = B_0 A \Rightarrow A|A_0$$

Ce qui prouve que A et A_0 sont associés et par suite il existe $\alpha \in K^*$ tel que $A = \alpha A_0$.

Par suite on a : $\alpha A_0 = A_0 D$.

$$\begin{cases} A \neq 0 \\ A_0 \sim A \end{cases} \Rightarrow A_0 \neq 0. \text{ Donc : } D = \alpha \in K^*.$$

Ce qui montre que A et B sont premiers entre eux.

Corollaire 4-3-2 :

Soient A , B et C des polynômes à coefficients dans K .

Si A et B sont premiers à C alors le produit A est premier à BC .

$$\text{C'est à dire : } \begin{cases} A \wedge B = 1 \\ A \wedge C = 1 \end{cases} \Rightarrow A \wedge BC = 1.$$

Démonstration :

Supposons que A est premiers à B et C .

- **Si $A = 0$:**

$$\begin{cases} B \sim 0 \wedge B = A \wedge B = 1 \\ C \sim 0 \wedge C = A \wedge C = 1 \end{cases} \Rightarrow B, C \in K^* \Rightarrow A \wedge BC = 1.$$

- **Si $A \neq 0$:**

Soit D un polynôme à coefficients dans K tel que A soit un diviseur de $(BC)D$.

Alors A est un diviseur de $B(CD)$.

$$\left\{ \begin{array}{l} A \neq 0 \\ A \wedge B = 1 \Rightarrow A|CD \Rightarrow A|D \text{ (car } A \neq 0 \text{ et } A \wedge C = 1). \\ A|B(CD) \end{array} \right.$$

Donc A est premier à BC .

Corollaire 4-3-3 :

Soient $A, B_1, B_2, \dots, B_n$ des polynômes à coefficients dans K .

Si A est premier à chacun des polynômes $B_1, B_2, \dots, B_n$ alors A est premier au produit $B_1 B_2 \dots B_n$.

C'est à dire : $[\forall k = 1, 2, \dots, n : A \wedge B_k = 1] \Rightarrow A \wedge (B_1 B_2 \dots B_n) = 1$.

$$\text{C'est à dire encore : } \left\{ \begin{array}{l} A \wedge B_1 = 1 \\ A \wedge B_2 = 1 \\ \dots\dots\dots \\ A \wedge B_n = 1 \end{array} \right. \Rightarrow A \wedge (B_1 B_2 \dots B_n) = 1.$$

Démonstration :

Montrons par récurrence sur $n \in \mathbb{N}^*$ que si $A, B_1, B_2, \dots, B_n \in K[X]$ et si A est premier à chacun des polynômes $B_1, \dots, B_n$ alors A est premier à $\prod_{k=1}^n B_k$.

- **Pour $n = 1$:**

Si $A, B_1 \in K[X]$ et si A est premier à B_1 alors A est premier à $B_1 = \prod_{k=1}^1 B_k = \prod_{k=1}^n B_k$.

- **Pour $n - 1$:**

Supposons que si $A, B_1, B_2, \dots, B_{n-1} \in K[X]$ et si A est premier à chacun des polynômes $B_1, \dots, B_{n-1}$ alors A est premier à $\prod_{k=1}^{n-1} B_k$.

- **Pour n :**

Montrons qu'alors si $A, B_1, B_2, \dots, B_n \in K[X]$ et si A est premier à chacun des polynômes $B_1, \dots, B_n$ alors A est premier à $\prod_{k=1}^n B_k$.

Soient $A, B_1, B_2, \dots, B_n \in K[X]$ tels que A soit premier à chacun des polynômes $B_1, \dots, B_n$.

Puisque A est premier à chacun des polynômes $B_1, \dots, B_{n-1}$ alors, d'après

l'hypothèse, A est premier à $\prod_{k=1}^{n-1} B_k$.

Donc A est premier à $\prod_{k=1}^n B_k = \left(\prod_{k=1}^{n-1} B_k \right) B_n$ (car A est premier à $\prod_{k=1}^{n-1} B_k$ et à B_n).

Corollaire 4-3-4 :

Soient $A_1, A_2, \dots, A_n, B_1, B_2, \dots, B_m$ des polynômes à coefficients dans K .
 Si chacun des polynômes $A_1, A_2, \dots, A_n$ est premier à chacun des polynômes $B_1, B_2, \dots, B_m$ alors le produit $A_1 A_2 \dots A_n$ est premier au produit $B_1 B_2 \dots B_m$.

Démonstration :

On suppose que chacun des polynômes $A_1, A_2, \dots, A_n$ est premier à chacun des polynômes $B_1, B_2, \dots, B_m$.

Alors (d'après le corollaire 4-3-3) chacun des polynômes $A_1, A_2, \dots, A_n$ est premier au produit $B_1 B_2 \dots B_m$.

Puisque le produit $B_1 B_2 \dots B_m$ est premier à chacun des polynômes $A_1, A_2, \dots, A_n$ alors (d'après le corollaire 4-3-3) le produit $B_1 B_2 \dots B_m$ est premier au produit $A_1 A_2 \dots A_n$.
 Ce qui montre que le produit $A_1 A_2 \dots A_n$ est premier au produit $B_1 B_2 \dots B_m$.

Corollaire 4-3-5 :

Soient A et B deux polynômes à coefficients dans K .

Si A et B sont premiers entre eux alors : $\forall n, m \in \mathbb{N} : A^n \wedge B^m = 1$.

C'est à dire : $A \wedge B = 1 \Rightarrow [\forall n, m \in \mathbb{N} : A^n \wedge B^m = 1]$.

Démonstration :

Supposons que A et B sont premiers entre eux et soient n, m deux entiers naturels quelconques.

- **Si $n = 0$:**

Alors : $A^n \wedge B^m = A^0 \wedge B^m = 1 \wedge B^m = 1$.

- **Si $m = 0$:**

Alors : $A^n \wedge B^m = A^n \wedge B^0 = A^n \wedge 1 = 1$.

- **Si $n \neq 0$ et si $m \neq 0$:**

Posons $A_1 = A_2 = \dots = A_n = A$ et $B_1 = B_2 = \dots = B_m = B$.

Puisque A et B sont premiers entre eux alors chacun des polynômes $A_1, A_2, \dots, A_n$ est premier à chacun des polynômes $B_1, B_2, \dots, B_m$.

Ce qui montre (d'après le corollaire 4-3-4) que :

$$A^n \wedge B^m = \left(\prod_{k=1}^n A_k \right) \wedge \left(\prod_{k=1}^m B_k \right) = 1.$$

Corollaire 4-3-6 :

Si $a, b \in K$ et si $a \neq b$ alors : $\forall n, m \in \mathbb{N} : (X - a)^n \wedge (X - b)^m = 1$.

Démonstration :

Soient a et b deux éléments distincts de K .

Puisque (d'après le corollaire 4-2-2) $X - a$ et $X - b$ sont premiers entre eux alors, d'après 4-3-5 on a : $\forall n, m \in \mathbb{N} : (X - a)^n \wedge (X - b)^m = 1$.

Corollaire 4-3-7 :

Soient A, P, Q des polynômes à coefficients dans K .

Si P et Q sont des diviseurs de A et si P et Q sont premiers entre eux alors le produit PQ est un diviseur de A .

Démonstration :

Supposons que P et Q sont des diviseurs de A et que P et Q sont premiers entre eux.

- **Si $A = 0$:**

Alors le produit PQ est un diviseur de $0 = A$.

- **Si $A \neq 0$:**

Alors P et Q sont non nuls (car P et Q sont des diviseurs de A).

Il existe un polynôme A_1 à coefficients dans K tels que : $A = PA_1$.

$$\begin{cases} Q \neq 0 \\ Q \wedge P = 1 \Rightarrow Q|A_1 \text{ (d'après l'identité de Gauss).} \\ Q|PA_1 \end{cases}$$

Donc il existe un polynôme A_2 à coefficients dans K tels que : $A_1 = QA_2$.

Par suite $A = PQA_2$. Ce qui montre que PQ est un diviseur de A .

Corollaire 4-3-8 :

Soient $A, P_1, P_2, \dots, P_n$ des polynômes à coefficients dans K .

Si $P_1, P_2, \dots, P_n$ sont des diviseurs de A et si $P_1, P_2, \dots, P_n$ sont premiers entre eux deux à deux alors le produit $P_1 P_2 \dots P_n$ est un diviseur de A .

Démonstration :

Montrons par récurrence sur $n \geq 2$ que si $A, P_1, P_2, \dots, P_n \in K[X]$, si $P_1, P_2, \dots, P_n$ sont des diviseurs de A et si $P_1, P_2, \dots, P_n$ sont premiers entre eux deux à deux alors le produit $P_1 P_2 \dots P_n$ est un diviseur de A .

- **Pour $n = 2$:**

Soient $A, P_1, P_2 \in K[X]$ tels que P_1, P_2 sont des diviseurs de A et tels P_1, P_2 sont premiers entre eux alors (d'après le corollaire 4-3-7) le produit $P_1 P_2$ est un diviseur de A .

- **Pour $n - 1$:**

Supposons que si $A, P_1, P_2, \dots, P_{n-1} \in K[X]$, si $P_1, P_2, \dots, P_{n-1}$ sont des diviseurs de A et si $P_1, P_2, \dots, P_{n-1}$ sont premiers entre eux deux à deux alors le produit $P_1 P_2 \dots P_{n-1}$ est un diviseur de A .

- **Pour n :**

Montrons qu'alors si $A, P_1, P_2, \dots, P_n \in K[X]$, si $P_1, P_2, \dots, P_n$ sont des diviseurs de A et si $P_1, P_2, \dots, P_n$ sont premiers entre eux deux à deux alors le produit $P_1 P_2 \dots P_n$ est un diviseur de A .

Soient $A, P_1, P_2, \dots, P_n \in K[X]$ tels que $P_1, P_2, \dots, P_n$ soient des diviseurs de A et tels que $P_1, P_2, \dots, P_n$ soient premiers entre eux deux à deux.

Puisque $P_1, P_2, \dots, P_{n-1}$ sont des diviseurs de A et puisque $P_1, P_2, \dots, P_{n-1}$ sont premiers entre eux deux à deux alors (d'après l'hypothèse de récurrence) le produit $P_1 P_2 \dots P_{n-1}$ est un diviseur de A .

D'après le corollaire 4-3-3, P_n est premier au produit $P_1 P_2 \dots P_{n-1}$ (car P_n est premier à chacun des polynômes $P_1, P_2, \dots, P_{n-1}$).

Par suite (d'après le corollaire 4-3-7) le produit $P_1 P_2 \dots P_n = (P_1 P_2 \dots P_{n-1}) P_n$ est un diviseur de A (car $P_1 P_2 \dots P_{n-1}$ et P_n sont des diviseurs de A premiers entre eux).

Corollaire 4-3-9 :

Soit A un polynôme à coefficients dans K .

Si $a_1, a_2, \dots, a_n$ sont des racines distinctes de A alors $(X - a_1)(X - a_2) \dots (X - a_n)$ est un diviseur de A .

Démonstration :

Supposons: que $a_1, a_2, \dots, a_n$ sont des racines distinctes de A .

Alors $X - a_1, X - a_2, \dots, X - a_n$ sont des diviseurs de A premiers entre eux.

Donc (d'après le corollaire 4-3-8), le produit $(X - a_1)(X - a_2) \dots (X - a_n)$ est un diviseur de A .

Corollaire 4-3-10 :

Soit A un polynôme non nul à coefficients dans K .

Le nombre des racines de A est fini et si r est le nombre des racines de A

alors : $r \leq d^0 A$.

Démonstration :

Posons $d^0(A) = n, A \neq 0 \Rightarrow n \in \mathbb{N}$.

Supposons que A admet au moins $n + 1$ racines $\alpha_1, \dots, \alpha_{n+1} \in K$.

Alors (d'après le corollaire 4-3-9) $\prod_{k=1}^{n+1} (X - \alpha_k)$ est un diviseur de A .

Par suite on a : $n + 1 = d^0 \left(\prod_{k=1}^{n+1} (X - \alpha_k) \right) \leq d^0(A) = n$. Ce qui est absurde.

Donc le nombre des racines de A est fini et si r est le nombre des racines de A alors $r \leq d^0(A) = n$.

Corollaire 4-3-11 :

Soient A un polynôme à coefficients dans $K, a_1, a_2, \dots, a_n \in K$ distinctes deux à deux et $k_1, k_2, \dots, k_n \in \mathbb{N}$ des entiers naturels.

Si $(X - a_1)^{k_1}, (X - a_2)^{k_2}, \dots, (X - a_n)^{k_n}$ sont des diviseurs de A alors le produit $(X - a_1)^{k_1} (X - a_2)^{k_2} \dots (X - a_n)^{k_n}$ est un diviseur de A .

Démonstration :

Supposons que $(X - a_1)^{k_1}, (X - a_2)^{k_2}, \dots, (X - a_n)^{k_n}$ sont des diviseurs de A .

Puisque (d'après le corollaire 4-2-2) $X - a_1, X - a_2, \dots, X - a_n$ sont premiers entre eux deux à deux alors (d'après le corollaire 4-3-6) $(X - a_1)^{k_1}, (X - a_2)^{k_2}, \dots, (X - a_n)^{k_n}$ sont premiers entre eux deux à deux.

Ce qui montre (d'après le corollaire 4-3-8) que le produit $(X - a_1)^{k_1} (X - a_2)^{k_2} \dots (X - a_n)^{k_n}$ est un diviseur de A (car $(X - a_1)^{k_1}, (X - a_2)^{k_2}, \dots, (X - a_n)^{k_n}$ sont des diviseurs de A premiers entre eux deux à deux).

4-4-p.p.c.m de deux polynômes :**Définition 4-4-1 :**

Soient A, B et M des polynômes à coefficients dans K .

On dit que M est un p.p.c.m de A et B si on a les deux propriétés suivantes :

- i) M est un multiple commun de A et B . C'est à dire : $\begin{cases} A|M \\ B|M \end{cases}$.
- ii) Tous les multiples communs de A et B sont des multiples de M .

$$\text{C'est à dire } \forall N \in K[X] : \begin{cases} A|N \\ B|N \end{cases} \Rightarrow M|N.$$

Propriétés 4-4-2 :

Soient A, B des polynômes à coefficients dans K .

1) Pour qu'un polynôme $M \in K[X]$ soit un $p.p.c.m$ de A et B il faut et il suffit que :

$$A \cdot K[X] \cap B \cdot K[X] = M \cdot K[X].$$

2) A et B possèdent au moins un $p.p.c.m$.

3) Si M est un $p.p.c.m$ de A et B alors les $p.p.c.m$ de A et B sont les associés de M .

C'est à dire si M est un $p.p.c.m$ de A et B alors pour tout polynôme $N \in K[X]$,
 $[N \text{ est un } p.p.c.m \text{ de } A \text{ et } B] \Leftrightarrow N \sim M$.

4) Si $K = \mathbb{C}$ et si M est un $p.p.c.m$ de A et B alors $\bar{M}$ est un $p.p.c.m$ de $\bar{A}$ et $\bar{B}$.

5) A est un $p.p.c.m$ de A et B si et seulement si $B|A$.

6) 0 est un $p.p.c.m$ de A et 0.

7) 0 est un $p.p.c.m$ de A et B si et seulement si $A = 0$ ou $B = 0$
et dans ce cas 0 est le seul $p.p.c.m$ de A et B .

8) Si $A = 0$ ou $B = 0$ alors 0 est le seul $p.p.c.m$ de A et B .

9) $\forall \alpha \in K^* : A$ est un $p.p.c.m$ de A et α .

Démonstration :

1) Soit M un polynôme à coefficients dans K .

$\Rightarrow$) Si M est un $p.p.c.m$ de A et B :

★ Puisque M est un $p.p.c.m$ de A et B alors M est un multiple commun de A et B ,

$$\text{donc : } \begin{cases} M \cdot K[X] \subset A \cdot K[X] \\ M \cdot K[X] \subset B \cdot K[X] \end{cases} \Rightarrow M \cdot K[X] \subset (A \cdot K[X] \cap B \cdot K[X]).$$

★ Puisque K est un corps commutatif alors (d'après le théorème 3-5-3), $K[X]$ est un anneau principal, et par suite $A \cdot K[X] \cap B \cdot K[X]$ est un idéal principal de $K[X]$. Donc il existe $N \in K[X]$ tel que : $A \cdot K[X] \cap B \cdot K[X] = N \cdot K[X]$.

Alors (d'après la propriété 3-4-2-5-b)), N est un multiple commun de A et B .

Donc N est un multiple de M (car M est un $p.p.c.m$ de A et B).

Par conséquent : $A \cdot K[X] \cap B \cdot K[X] = N \cdot K[X] \subset M \cdot K[X]$.

Ce qui montre que $A \cdot K[X] \cap B \cdot K[X] = M \cdot K[X]$.

$\Leftarrow$) Si on a : $A \cdot K[X] \cap B \cdot K[X] = M \cdot K[X]$:

★ Puisque $M \cdot K[X] \subset M \cdot K[X] = A \cdot K[X] \cap B \cdot K[X]$, alors (d'après la propriété 3-4-2-5-b)) M est un multiple commun de A et B .

★ Soit N un multiple commun quelconque de A et B .

D'après la propriété 3-4-2-5-b), $N \cdot K[X] \subset A \cdot K[X] \cap B \cdot K[X] = M \cdot K[X]$.

Par suite N est un multiple de M .

Donc M est un $p.p.c.m$ de A et B .

Ce qui montre que M est un $p.p.c.m$ de A et B si et seulement si.

$$A \cdot K[X] \cap B \cdot K[X] = M \cdot K[X].$$

2) Puisque $A \cdot K[X] \cap B \cdot K[X]$ est un idéal principal de $K[X]$ alors il existe un polynôme

$M \in K[X]$ tel que : $A \cdot K[X] \cap B \cdot K[X] = M \cdot K[X]$.

Donc M est un $p.p.c.m$ de A et B .

3) Soit M est un $p.p.c.m$ de A et B , et soit N un polynôme quelconque à coefficients dans K

Puisque M est un $p.p.c.m$ de A et B alors (d'après 1)) on a :

$$A \cdot K[X] \cap B \cdot K[X] = M \cdot K[X].$$

$$[N \text{ est un } p.p.c.m \text{ de } A \text{ et } B] \Leftrightarrow A \cdot K[X] \cap B \cdot K[X] = N \cdot K[X] \text{ (d'après 1))}$$

$$\Leftrightarrow N \cdot K[X] = M \cdot K[X]$$

$$\Leftrightarrow N \sim M.$$

Donc les $p.p.c.m$ de A et B sont les associés de M .

4) Supposons que $K = \mathbb{C}$ et soit M un $p.p.c.m$ de A et B .

★ Puisque M est un multiple commun de A et B alors (d'après la propriété 3-4-2-1))

$\bar{M}$ est aussi un multiple commun de $\bar{A}$ et $\bar{B}$.

★ Soit N un multiple commun quelconque de $\bar{A}$ et $\bar{B}$.

Alors (d'après la propriété 3-4-2-1)) $\bar{N}$ est un multiple commun de $\bar{\bar{A}} = A$ et $\bar{\bar{B}} = B$.

Par suite $\bar{N}$ est un multiple de M (car M est un $p.p.c.m$ de A et B).

D'après la propriété 3-4-2-1)) on a donc $N = \bar{\bar{N}}$ est un multiple de $\bar{M}$.

Ce qui montre que $\bar{M}$ est un $p.p.c.m$ de $\bar{A}$ et $\bar{B}$.

$$5) [A \text{ est un } p.p.c.m \text{ de } A \text{ et } B] \Leftrightarrow A \cdot K[X] \cap B \cdot K[X] = A \cdot K[X] \Leftrightarrow A \cdot K[X] \subset B \cdot K[X] \\ \Leftrightarrow B|A.$$

6) Puisque 0 est un multiple de A alors (d'après 5)) 0 est un $p.p.c.m$ de 0 et A .

7) $\Rightarrow$) **Si 0 est un p.p.c.m de A et B :**

$$\begin{cases} A|(AB) \\ B|(AB) \end{cases} \Rightarrow 0|(AB) \text{ (car 0 est un } p.p.c.m \text{ de } A \text{ et } B) \Rightarrow AB = 0 \\ \Rightarrow [A = 0 \text{ ou } B = 0].$$

$\Leftarrow$) **Si A = 0 ou B = 0 :**

$$\text{On a : } A \cdot K[X] \cap B \cdot K[X] = \{0\} = 0 \cdot K[X].$$

Ce qui montre que 0 est un $p.p.c.m$ de A et B si seulement si $A = 0$ ou $B = 0$.

8) Supposons que $A = 0$ ou $B = 0$.

D'après 7), 0 est un $p.p.c.m$ de A et B .

Puisque 0 est le seul associé 0 alors 0 est le seul $p.p.c.m$ de A et B .

9) $\forall \alpha \in K^* : \alpha$ est un diviseur de A , donc d'après 5) A est un $p.p.c.m$ de A et α .

Théorème 4-4-3 :

Soient A et B deux polynômes à coefficients dans K et D un $p.g.c.d$ de A et B .

Si A_0 et B_0 sont deux polynômes à coefficients dans K tels que :

$$\begin{cases} A = A_0 D \\ B = B_0 D \\ A_0 \wedge B_0 = 1 \end{cases}$$

Alors $AB_0 = A_0 B$ est un $p.p.c.m$ de A et B .

Si en particulier $D \neq 0$ (c'est à dire si $A \neq 0$ ou $B \neq 0$) et si M est le quotient de la division euclidienne de AB par D alors $M = AB_0 = A_0 B$ est un $p.p.c.m$ de A et B .

Recherche :

Soient $A, B \in K[X]$ deux polynômes à coefficients dans K .

- **Si A = 0 ou B = 0 :**

Alors : 0 est un $p.p.c.m$ de A et B et c'est le seul $p.p.c.m$ de A et B

- **Si $A \neq 0$ et $B \neq 0$:**

On cherche d'abord un $p.g.c.d$, D de A et B puis on peut utiliser l'une des trois méthodes suivantes :

★ **1^{ère} méthode :**

On effectue la division euclidienne de B par D .
$$\begin{array}{r|l} B & D \\ 0 & B_0 \end{array}$$

Si B_0 est le quotient de la division euclidienne de B par D alors le produit AB_0 est un $p.p.c.m$ de A et B .

★ **2^{ème} méthode :**

On effectue la division euclidienne de A par D .
$$\begin{array}{r|l} A & D \\ 0 & A_0 \end{array}$$

Si A_0 est le quotient de la division euclidienne de A par D alors le produit A_0B le A_0B est un $p.p.c.m$ de A et B .

★ **3^{ème} méthode :**

On calcul le produit AB puis on effectue la division euclidienne de AB par D .

$$\begin{array}{r|l} AB & D \\ 0 & M \end{array}$$

Alors le quotient M de la division euclidienne de AB par D est un $p.p.c.m$ de A et B .

Démonstration :

• $AB_0 = (A_0DB_0) = A_0(DB_0) = A_0B.$

• - **Si $B = 0$:**

Alors $AB_0 = A_0B = 0$ est un $p.p.c.m$ de A et B .

- **Si $B \neq 0$:**

• $B = B_0D \neq 0 \Rightarrow [B_0 \neq 0 \text{ et } D \neq 0].$

• $AB_0 = A_0B$ est un multiple commun de A et B .

• Soit M un multiple commun de A et B .

Alors il existe deux polynômes $P, Q \in K[X]$ tels que : $M = AP = BQ.$

$B_0QD = B_0DQ = BQ = M = AP = A_0DP = A_0PD \Rightarrow B_0Q = A_0P \Rightarrow B_0|A_0P.$

$$\left\{ \begin{array}{l} B_0 \neq 0 \\ B_0 \wedge A_0 = 1 \Rightarrow B_0|P \Rightarrow \exists S \in K[X] \text{ tq : } P = B_0S. \\ B_0|A_0P \end{array} \right.$$

Donc : $M = AB_0S \Rightarrow AB_0|M.$

Ce qui montre que $AB_0 = A_0B$ est un $p.p.c.m$ de A et B .

Exemple 4-4-4 :

Dans $\mathbb{R}[X]$ soient $A = 8X^5 + 4X^4 + 10X^3 - 5X^2 + X - 1$ et $B = 4X^4 + 4X^3 + 5X^2 - 2X - 1.$

On a vu que $D = 2X - 1$ est un $p.g.c.d$ de A et B .

★ **1^{ère} méthode :**

$$\begin{array}{r|l} B = 4X^4 + 4X^3 + 5X^2 - 2X - 1 & D = 2X - 1 \\ 0 & B_0 = 2X^3 + 3X^2 + 4X + 1 \end{array}$$

$$AB_0 = (8X^5 + 4X^4 + 10X^3 - 5X^2 + X - 1)(2X^3 + 3X^2 + 4X + 1) \\ = 16X^8 + 32X^7 + 64X^6 + 44X^5 + 31X^4 - 9X^3 - 4X^2 - 3X - 1$$

est un *p.p.c.m* de A et B .

★ **2^{ème} méthode :**

$$\begin{array}{r|l} A = 8X^5 + 4X^4 + 10X^3 - 5X^2 + X - 1 & D = 2X - 1 \\ 0 & \overline{A_0 = 4X^4 + 4X^3 + 7X^2 + X + 1} \end{array}$$

$$A_0B = (4X^4 + 4X^3 + 7X^2 + X + 1)(4X^4 + 4X^3 + 5X^2 - 2X - 1) \\ = 16X^8 + 32X^7 + 64X^6 + 44X^5 + 31X^4 - 9X^3 - 4X^2 - 3X - 1$$

est un *p.p.c.m* de A et B .

★ **3^{ème} méthode :**

$$AB = (8X^5 + 4X^4 + 10X^3 - 5X^2 + X - 1)(4X^4 + 4X^3 + 5X^2 - 2X - 1) \\ = 32X^9 + 48X^8 + 96X^7 + 24X^6 + 18X^5 - 49X^4 + X^3 - 2X^2 + X + 1$$

On effectue la division euclidienne de AB par $D = 2X - 1$ on trouve que le reste est nul et que le quotient est :

$$M = 16X^8 + 32X^7 + 64X^6 + 44X^5 + 31X^4 - 9X^3 - 4X^2 - 3X - 1 \text{ est un } p.p.c.m \text{ de } A \text{ et } B. \\ \text{On a donc : } AB_0 = A_0B = M = 16X^8 + 32X^7 + 64X^6 + 44X^5 + 31X^4 - 9X^3 - 4X^2 - 3X - 1.$$

Propriétés 4-4-5 :

Soient A et B deux polynômes à coefficients dans K .

1) Soit M un polynôme à coefficients dans K et soit D un *p.g.c.d* de A et B .

a) Si M est un *p.p.c.m* de A et B alors MD est associé à AB .

C'est à dire si M est un *p.p.c.m* de A et B alors $MD \sim AB$.

b) Si $D \neq 0$ (c'est à dire si $A \neq 0$ ou $B \neq 0$) alors M est un *p.p.c.m* de A et B si seulement si MD est associé à AB .

C'est à dire si $A \neq 0$ ou si $B \neq 0$ alors : M est un *p.p.c.m* de A et $B \Leftrightarrow MD \sim AB$.

2) Si A et B sont premiers entre eux alors AB est un *p.p.c.m* de A et B .

C'est à dire : $A \wedge B = 1 \Rightarrow AB$ est un *p.p.c.m* de A et B .

3) Si $A \neq 0$ et si $B \neq 0$ alors A et B sont premiers entre eux si seulement si AB est un *p.p.c.m* de A et B .

C'est à dire si $A \neq 0$ et si $B \neq 0$ alors : $A \wedge B = 1 \Leftrightarrow AB$ est un *p.p.c.m* de A et B .

Démonstration :

1) Soient A_0 et B_0 deux polynômes à coefficients dans K tels que :
$$\begin{cases} A = A_0D \\ B = B_0D \\ A_0 \wedge B_0 = 1 \end{cases}.$$

a) Supposons que M est un *p.p.c.m* de A et B .

Alors M et AB_0 sont associés (car M et AB_0 sont des *p.p.c.m* de A et B).

Donc il existe un élément non $\alpha \in K$ tel que : $M = \alpha(AB_0)$.

Par suite : $MD = \alpha(AB_0)D = \alpha A(B_0D) = \alpha AB \Rightarrow MD \sim AB$.

b) Supposons que $D \neq 0$ (c'est à dire si $A \neq 0$ ou $B \neq 0$).

$\Rightarrow$) **Si M est un *p.p.c.m* de A et B :**

Alors (d'après a)) MD est associé à AB .

$\Leftarrow$) **Si MD est associé à AB :**

Alors il existe un élément non $\alpha \in K$ tel que : $MD = \alpha AB$.

Donc : $MD = \alpha AB_0 D \Rightarrow M = \alpha AB_0$ (car $D \neq 0$) $\Rightarrow M \sim AB_0$.

Ce qui montre que M est un $p.p.c.m$ de A et B .

2) Supposons que A et B sont premiers entre eux.

$AB(A \wedge B) = AB1 = AB \sim AB$. Donc (d'après 1) a)) AB est un $p.p.c.m$ de A et B .

3) Supposons que $A \neq 0$ et $B \neq 0$.

$\Rightarrow$) **Si A et B sont premiers entre eux :**

Alors (d'après 2)) AB est un $p.p.c.m$ de A et B .

$\Leftarrow$) **Si AB est un p.p.c.m de A et B :**

Alors (d'après 1) a)) :

$$\begin{aligned} AB(A \wedge B) \sim AB &\Rightarrow [\exists \alpha \in K^* \text{ tq : } AB(A \wedge B) = \alpha AB] \\ &\Rightarrow [\exists \alpha \in K^* \text{ tq : } A \wedge B = \alpha] \Rightarrow A \wedge B \in K^* \\ &\Rightarrow A \wedge B = 1 \text{ (car } A \wedge B \text{ est unitaire).} \end{aligned}$$

Proposition et définition 4-4-6 :

Soient A et B deux polynômes à coefficients dans K et M un $p.p.c.m$ quelconque de A et B .

- **Si $M \neq 0$ (c'est à dire si $A \neq 0$ et $B \neq 0$) :**

Alors A et B possèdent un $p.p.c.m$ unitaire et un seul noté $A \vee B$ appelé le $p.p.c.m$ de A et B .

Si α est le coefficient dominant de M alors : $A \vee B = \frac{1}{\alpha} M$

- **Si $M = 0$ (c'est à dire si $A = 0$ ou $B = 0$) :**

Alors 0 est le seul $p.p.c.m$ de A et B appelé le $p.p.c.m$ de A et B et on note $A \vee B = 0$.

En effet :

- **Si $M \neq 0$ (c'est à dire si $A \neq 0$ et $B \neq 0$) :**

Soit α le coefficient dominant de M .

Puisque $\frac{1}{\alpha} M$ est le seul polynôme unitaire de $K[X]$ associé à M alors $\frac{1}{\alpha} M$ est un $p.p.c.m$ unitaire de A et B , et c'est le seul $p.p.c.m$ unitaire de A et B .

- **Si $M = 0$ (c'est à dire si $A = 0$ ou $B = 0$) :**

Puisque 0 est le seul polynôme de $K[X]$ associé à lui même alors 0 est le seul $p.p.c.m$ de A et B .

Exemple 4-4-7 :

Dans $\mathbb{R}[X]$ soient $A = 8X^5 + 4X^4 + 10X^3 - 5X^2 + X - 1$ et $B = 4X^4 + 4X^3 + 5X^2 - 2X - 1$

$$\begin{aligned} A \vee B &= \frac{1}{16} (16X^8 + 32X^7 + 64X^6 + 44X^5 + 31X^4 - 9X^3 - 4X^2 - 3X - 1) \\ &= X^8 + 2X^7 + 4X^6 + \frac{11}{4}X^5 + \frac{31}{16}X^4 - \frac{9}{16}X^3 - \frac{1}{4}X^2 - \frac{3}{16}X - \frac{1}{16}. \end{aligned}$$

Remarque 4-4-8 :

Si A et B sont deux polynômes à coefficients dans K alors : $\overline{A \vee B} = \overline{A} \vee \overline{B}$.

En effet :

★ Si $A \vee B = 0$ alors $A = 0$ ou $B = 0$ et par suite $\overline{A} = 0$ ou $\overline{B} = 0$

$$\overline{A \vee B} = 0 = \overline{A \wedge B}.$$

★ Si $A \vee B \neq 0$ alors :

$$\begin{cases} A \vee B \text{ est un p.p.c.m de } A \text{ et } B \\ A \vee B \text{ est unitaire} \end{cases} \Rightarrow \begin{cases} \overline{A \vee B} \text{ est un p.p.c.m de } A \text{ et } B \\ \overline{A \vee B} \text{ est unitaire} \end{cases}$$

$$\Rightarrow \overline{A} \vee \overline{B} = \overline{A \vee B}.$$

Proposition :

Soient A et B deux polynômes non nuls à coefficients dans K .

Si a est le coefficient dominant de A et si b est le coefficient dominant de B alors :

$$AB = ab(A \vee B)(A \wedge B)$$

En effet :

Supposons que a est le coefficient dominant de A et si b est le coefficient dominant de B .
Puisque $A \vee B$ est un p.p.c.m de A et B et puisque $A \wedge B$ est un p.g.c.d de A et B alors, d'après la propriété 4-4-5-1) a), $(A \vee B)(A \wedge B)$ est associé à AB .

Donc : $\exists \alpha \in K^*$ tq : $AB = \alpha(A \vee B)(A \wedge B)$.

Puisque $(A \vee B)(A \wedge B)$ est unitaire et puisque ab est le coefficient dominant de AB alors $\alpha = ab$.

Ce qui montre que : $AB = ab(A \vee B)(A \wedge B)$.

4-5-Polynômes irréductibles :

Définition 4-5-1 :

Soient P un polynôme à coefficients dans K .

On dit que P est irréductible dans $K[X]$ ou P est irréductible si $d^0 P \geq 1$ et si les seuls diviseurs de P dans $K[X]$ sont les constantes non nulles de K et les associés de P dans $K[X]$. C'est à dire :

$$P \text{ est irréductible dans } K[X] \Leftrightarrow \begin{cases} d^0 P \geq 1 \\ \forall Q \in K[X] : Q|P \Rightarrow [Q \in K^* \text{ ou } Q \sim P] \end{cases}.$$

Propriétés 4-5-2 :

1) Tous les polynômes de degré 1 à coefficients dans K sont irréductibles dans $K[X]$

C'est à dire : $\forall P \in K[X] : d^0 P = 1 \Rightarrow P$ est irréductible dans $K[X]$.

2) Tous les associés dans $K[X]$ d'un polynôme irréductible dans $K[X]$ sont irréductibles dans $K[X]$ C'est à dire : $\forall P, Q \in K[X] :$

$$\begin{cases} P \in K[X] \text{ est irréductible dans } K[X] \\ P \sim Q \end{cases} \Rightarrow Q \text{ est irréductible dans } K[X].$$

3) Soient A un polynôme à coefficients dans K et P un polynôme irréductible dans $K[X]$.

a) $P|A \Leftrightarrow P \wedge A \neq 1$.

b) $P \wedge A = 1 \Leftrightarrow P \nmid A$.

4) Soient $P, Q \in K[X]$ deux polynômes irréductibles dans $K[X]$.

a) $P \sim Q \Leftrightarrow P|Q \Leftrightarrow P \wedge Q \neq 1$.

b) $[P \text{ et } Q \text{ ne sont pas associés}] \Leftrightarrow P \nmid Q \Leftrightarrow P \wedge Q = 1$.

- c) Si P et Q sont unitaires alors :
 $P = Q \Leftrightarrow P \sim Q \Leftrightarrow P|Q \Leftrightarrow P \wedge Q \neq 1.$
- d) Si P et Q sont unitaires alors :
 $P \neq Q \Leftrightarrow [P \text{ et } Q \text{ ne sont pas associés}] \Leftrightarrow P \not\sim Q \Leftrightarrow P \wedge Q = 1.$
- e) Si P et Q ne sont pas associés alors :
 $\forall n, m \in \mathbb{N} : P^n \wedge Q^m = 1.$
- f) Si P et Q sont unitaires et si $P \neq Q$ alors :
 $\forall n, m \in \mathbb{N} : P^n \wedge Q^m = 1.$
- 5) Soit $P \in K[X]$ un polynôme irréductible dans $K[X]$.
- a) $\forall A, B \in K[X] : P|(AB) \Rightarrow [P|A \text{ ou } P|B].$
- b) $\forall A_1, A_2, \dots, A_n \in K[X] : P|(A_1 A_2 \dots A_n) \Rightarrow [\exists k = 1, 2, \dots, n \text{ tq : } P|A_k].$
- c) $\forall A \in K[X] \quad \forall n \in \mathbb{N} : P|A^n \Rightarrow \begin{cases} n \geq 1 \\ P|A \end{cases}.$
- d) Si $P_1, P_2, \dots, P_n$ sont des polynômes irréductibles dans $K[X]$ et si P est un diviseur du produit $P_1 P_2 \dots P_n$ alors il existe un entier naturel $k = 1, 2, \dots, n$ tel que P soit associé à P_k .
- e) Si Q est un polynôme irréductible dans $K[X]$ et si n est un entier naturel alors :
 $P|Q^n \Rightarrow \begin{cases} n \geq 1 \\ P \sim Q \end{cases}.$
- f) Si P est unitaire et si $P_1, P_2, \dots, P_n$ sont des polynômes irréductibles unitaire dans $K[X]$ alors : $P|(P_1 P_2 \dots P_n) \Rightarrow [\exists k = 1, 2, \dots, n \text{ tq : } P = P_k].$
- g) Si P est unitaire, Q est un polynôme irréductible unitaire dans $K[X]$ et n est un entier naturel alors : $P|Q^n \Rightarrow \begin{cases} n \geq 1 \\ P = Q \end{cases}.$
- 6) Soient $A \in K[X]$ un polynôme à coefficients dans K et $P_1, P_2, \dots, P_n \in K[X]$ des polynômes irréductibles dans $K[X]$.
- a) Si $P_1, P_2, \dots, P_n$ sont des diviseurs de A et si $P_1, P_2, \dots, P_n$ ne sont pas associés deux à deux alors le produit $P_1 P_2 \dots P_n$ est un diviseur de A .
- b) Si $P_1, P_2, \dots, P_n$ sont des diviseurs de A et si $P_1, P_2, \dots, P_n$ sont unitaires distincts deux à deux alors le produit $P_1 P_2 \dots P_n$ est un diviseur de A .
- c) Soient $k_1, k_2, \dots, k_n \in \mathbb{N}$ des entiers naturels.
Si $P_1^{k_1}, P_2^{k_2}, \dots, P_n^{k_n}$ sont des diviseurs de A et si $P_1, P_2, \dots, P_n$ ne sont pas associés deux à deux alors le produit $P_1^{k_1} P_2^{k_2} \dots P_n^{k_n}$ est un diviseur de A .
- d) Soient $k_1, k_2, \dots, k_n \in \mathbb{N}$ des entiers naturels.
Si $P_1^{k_1}, P_2^{k_2}, \dots, P_n^{k_n}$ sont des diviseurs de A et si $P_1, P_2, \dots, P_n$ sont unitaires distincts deux à deux alors le produit $P_1^{k_1} P_2^{k_2} \dots P_n^{k_n}$ est un diviseur de A .
- 7) Si $A \in K[X]^*$ est un polynôme non nul à coefficients dans K , le nombre des diviseurs irréductibles unitaires de A est fini et si r est le nombre des diviseurs irréductibles de A alors, $r \leq d^0 A$.

Démonstration :

1) Supposons que P est un polynôme de degré 1 à coefficients dans K .

Soit Q un diviseur quelconque de P Il existe alors un polynôme S à coefficients dans K tel que $P = QS$.

$$\begin{cases} P \neq 0 \\ Q|P \end{cases} \Rightarrow d^0 Q \leq d^0 P = 1 \Rightarrow [d^0 Q = 0 \text{ ou } d^0 Q = 1].$$

- Si $d^0 Q = 0$:

Alors Q est une constante non nulle.

- Si $d^0 Q = 1$:

$$\begin{cases} Q|P \\ d^0 Q = 1 = d^0 P \end{cases} \Rightarrow Q \sim P.$$

Donc P est un polynôme irréductible dans $K[X]$.

2) Supposons que P est un polynôme irréductible dans $K[X]$ et Q est un polynôme à coefficients dans K associé à P .

Soit S un diviseur quelconque de Q

$$\begin{cases} S|Q \\ Q \sim P \end{cases} \Rightarrow \begin{cases} S|Q \\ Q|P \end{cases} \Rightarrow S|P \Rightarrow [S \in K^* \text{ ou } S \sim P] \\ \Rightarrow [S \in K^* \text{ ou } S \sim Q] \text{ (car } Q \sim P).$$

3) a) $\Rightarrow$) Si $P|A$:

Alors P est un p.g.c.d de P et A . Donc $P \wedge A \neq 1$ (car $P \notin K$).

$\Leftarrow$) Si $P \wedge A \neq 1$:

$$\begin{cases} (P \wedge A)|P \\ P \wedge A \neq 1 \end{cases} \Rightarrow \begin{cases} (P \wedge A)|P \\ (P \wedge A) \notin K \end{cases} \Rightarrow (P \wedge A) \sim P \\ \Rightarrow [P \text{ est un p.g.c.d de } P \text{ et } A] \\ \Rightarrow P|A.$$

$$b) [P|A \Leftrightarrow P \wedge A \neq 1] \Rightarrow [non(P \wedge A \neq 1) \Leftrightarrow non(P|A)] \Rightarrow [P \wedge A = 1 \Leftrightarrow P \nmid A].$$

$$4) a) P \sim Q \Leftrightarrow \begin{cases} P|Q \\ P \notin K^* \end{cases} \text{ (car } Q \text{ est un polynôme irréductible dans } K[X]) \\ \Leftrightarrow P|Q. \text{ (car } P \notin K^*).$$

$$P \sim Q \Leftrightarrow P|Q \Leftrightarrow P \wedge Q \neq 1 \text{ (d'après 3) b)}$$

$$b) \text{ D'après a) on a : } [non(P \sim Q)] \Leftrightarrow non(P|Q) \Leftrightarrow non(P \wedge Q \neq 1).$$

$$\text{Par suite on a : } [P \text{ et } Q \text{ ne sont pas associés}] \Leftrightarrow P \nmid Q \Leftrightarrow P \wedge Q = 1.$$

c) Si P et Q sont unitaires alors (d'après b)) :

$$P = Q \Leftrightarrow P \sim Q \Leftrightarrow P|Q \Leftrightarrow P \wedge Q \neq 1.$$

d) Si P et Q sont unitaires alors (d'après c) :

$$non(P = Q) \Leftrightarrow non(P \sim Q) \Leftrightarrow non(P|Q) \Leftrightarrow non(P \wedge Q \neq 1).$$

$$\text{On a donc : } P \neq Q \Leftrightarrow [P \text{ et } Q \text{ ne sont pas associés}] \Leftrightarrow P \nmid Q \Leftrightarrow P \wedge Q = 1.$$

e) Supposons que P et Q ne sont pas associés.

$$\text{Alors (d'après b)) : } P \wedge Q = 1 \Rightarrow [\forall n, m \in \mathbb{N} : P^n \wedge Q^m = 1].$$

f) Supposons que P et Q sont unitaires et que $P \neq Q$ alors :

$$\text{Alors (d'après c)) : } P \wedge Q = 1 \Rightarrow [\forall n, m \in \mathbb{N} : P^n \wedge Q^m = 1].$$

5) a) Soient A et B deux polynômes à coefficients dans K tels que P soit un diviseur de AB .

Supposons que P ne divise ni A ni B .

$$\begin{cases} P \nmid A \\ P \nmid B \end{cases} \Rightarrow \begin{cases} P \wedge A = 1 \\ P \wedge B = 1 \end{cases} \Rightarrow P \wedge (AB) = 1.$$

$$\begin{cases} P \neq 0 \\ P \wedge (AB) = 1 \Rightarrow P|1 \Rightarrow P \in K^*. \text{ Ce qui est absurde (car } P \text{ est irréductible).} \\ P|(AB)1 \end{cases}$$

Ce qui montre que $P|A$ ou $P|B$.

b) Montrons par récurrence sur $n \geq 2$ que : $\forall A_1, A_2, \dots, A_n \in K[X]$:

$$P|(A_1 A_2 \dots A_n) \Rightarrow [\exists k = 1, 2, \dots, n \text{ tq : } P|A_k].$$

- **Pour $n = 2$:**

$$\begin{aligned} \forall A_1, A_2 \in K[X] : P|(A_1 A_2) &\Rightarrow [P|A_1 \text{ ou } P|A_2] \text{ (d'après a)} \\ &\Rightarrow [\exists k = 1, 2 \text{ tq : } P|A_k] \\ &\Rightarrow [\exists k = 1, 2, \dots, n \text{ tq : } P|A_k]. \end{aligned}$$

- **Pour $n - 1$:**

Supposons que : $\forall A_1, A_2, \dots, A_{n-1} \in K[X]$:

$$P|(A_1 A_2 \dots A_{n-1}) \Rightarrow [\exists k = 1, 2, \dots, n-1 \text{ tq : } P|A_k].$$

- **Pour n :**

Montrons qu'alors : $\forall A_1, A_2, \dots, A_n \in K[X]$:

$$P|(A_1 A_2 \dots A_n) \Rightarrow [\exists k = 1, 2, \dots, n \text{ tq : } P|A_k].$$

Soient $A_1, A_2, \dots, A_n \in K[X]$ tels que P un diviseur du produit $A_1 A_2 \dots A_n$.

$$\begin{aligned} P|(A_1 A_2 \dots A_n) &\Rightarrow P|[(A_1 A_2 \dots A_{n-1}) A_n] \\ &\Rightarrow [P|(A_1 A_2 \dots A_{n-1}) \text{ ou } P|A_n] \text{ (d'après a)} \\ &\Rightarrow [[\exists k = 1, 2, \dots, n-1 \text{ tq : } P|A_k] \text{ ou } P|A_n] \\ &\Rightarrow [\exists k = 1, 2, \dots, n \text{ tq : } P|A_k]. \end{aligned}$$

c) Soient $A \in K[X]$ et n un entier naturel. On suppose que P est un diviseur de A^n .

Puisque P est un polynôme irréductible dans $K[X]$ alors $P \notin K$.

$$P \notin K \Rightarrow P \nmid 1 \Rightarrow P \nmid A^0 \Rightarrow n \neq 0 \Rightarrow n \geq 1.$$

Posons : $A_1 = A_2 = \dots = A_n = A$. Alors : $A^n = A_1 A_2 \dots A_n$.

$$\text{On a donc : } P|A^n \Rightarrow \begin{cases} n \geq 1 \\ P|(A_1 A_2 \dots A_n) \end{cases} \Rightarrow \begin{cases} n \geq 1 \\ \exists k = 1, 2, \dots, n \text{ tq : } P|A_k \end{cases}$$

$$\Rightarrow \begin{cases} n \geq 1 \\ P|A \end{cases}.$$

d) Supposons que $P_1, P_2, \dots, P_n$ sont des polynômes irréductibles dans $K[X]$ et que P est un diviseur du produit $P_1 P_2 \dots P_n$.

$$\begin{aligned} P|(P_1 P_2 \dots P_n) &\Rightarrow [\exists k = 1, 2, \dots, n \text{ tq : } P|P_k] \\ &\Rightarrow [\exists k = 1, 2, \dots, n \text{ tq : } P \sim P_k] \text{ (d'après 4) a)}. \end{aligned}$$

e) Supposons que Q est un polynôme irréductible dans $K[X]$ et que n est un entier

$$\text{naturel. } P|Q^n \Rightarrow \begin{cases} n \geq 1 \\ P|Q \end{cases} \Rightarrow \begin{cases} n \geq 1 \\ P \sim Q \end{cases}.$$

f) Supposons que P est unitaire, que $P_1, P_2, \dots, P_n$ sont des polynômes irréductibles unitaire dans $K[X]$ et que P est un diviseur du produit $P_1 P_2 \dots P_n$.

$$P|(P_1 P_2 \dots P_n) \Rightarrow [\exists k = 1, 2, \dots, n \text{ tq : } P \sim P_k] \text{ (d'après d))} \\ \Rightarrow [\exists k = 1, 2, \dots, n \text{ tq : } P = P_k].$$

g) Supposons que P est unitaire, Q est un polynôme irréductible unitaire dans $K[X]$, n est un entier naturel P est un diviseur de Q^n .

$$P|Q^n \Rightarrow \begin{cases} n \geq 1 \\ P \sim Q \end{cases} \text{ (d'après e))} \Rightarrow \begin{cases} n \geq 1 \\ P = Q \end{cases} \text{ (car } P \text{ et } Q \text{ sont unitaires).}$$

6) a) Supposons que $P_1, P_2, \dots, P_n$ sont des diviseurs de A et que $P_1, P_2, \dots, P_n$ ne sont pas associés deux à deux.

Puisque $P_1, \dots, P_n$ sont des polynômes irréductibles dans $K[X]$ non associés deux à deux, alors $P_1, \dots, P_n$ sont des diviseurs de A premiers entre eux deux à deux. Donc le produit $P_1 P_2 \dots P_n$ est un diviseur de A .

b) Supposons que $P_1, P_2, \dots, P_n$ sont des diviseurs de A et que $P_1, P_2, \dots, P_n$ sont unitaires.

Puisque $P_1, \dots, P_n$ sont des polynômes irréductibles unitaires dans $K[X]$, distincts deux à deux, alors $P_1, \dots, P_n$ sont des diviseurs irréductibles de A non associés deux à deux.

Donc (d'après a)) le produit $P_1 P_2 \dots P_n$ est un diviseur de A .

c) Supposons que $P_1^{k_1}, P_2^{k_2}, \dots, P_n^{k_n}$ sont des diviseurs de A et que $P_1, P_2, \dots, P_n$ ne sont pas associés deux à deux.

Puisque $P_1, P_2, \dots, P_n$ sont des polynômes irréductibles dans $K[X]$ non associés deux à deux, alors $P_1, P_2, \dots, P_n$ sont premiers entre eux deux à deux.

Donc $P_1^{k_1}, P_2^{k_2}, \dots, P_n^{k_n}$ sont premiers entre eux deux à deux.

Par suite $P_1^{k_1}, P_2^{k_2}, \dots, P_n^{k_n}$ sont des diviseurs de A , premiers entre eux deux à deux.

Donc le produit $P_1^{k_1} P_2^{k_2} \dots P_n^{k_n}$ est un diviseur de A .

d) Supposons que $P_1^{k_1}, P_2^{k_2}, \dots, P_n^{k_n}$ sont des diviseurs de A et que $P_1, P_2, \dots, P_n$ sont unitaires distincts deux à deux.

Puisque $P_1, P_2, \dots, P_n$ sont des polynômes irréductibles unitaires dans $K[X]$ distincts deux à deux alors $P_1, P_2, \dots, P_n$ sont des polynômes irréductibles dans $K[X]$ non associés deux à deux.

Donc (d'après c)) le produit $P_1^{k_1} P_2^{k_2} \dots P_n^{k_n}$ est un diviseur de A .

7) Soit A est un polynôme non nul à coefficients dans K . Posons $d^0 A = n$.

Supposons que A admet au moins $n + 1$ diviseurs irréductibles unitaires $P_1, P_2, \dots, P_{n+1}$ de A distincts deux à deux.

D'après 6) b), le produit $P_1 P_2 \dots P_{n+1}$ est un diviseur de A .

$$\text{Donc : } n + 1 \leq d^0(P_1) + d^0(P_2) + \dots + d^0(P_{n+1}) = d^0(P_1 P_2 \dots P_{n+1}) \leq d^0 A = n.$$

Ce qui est absurde.

Par la suite le nombre des diviseurs irréductibles de A est fini et que si r est le nombre des diviseurs irréductibles unitaires de A alors, $r \leq d^0 A$.

Théorème 4-5-3 :

Tous les polynômes non constants à coefficients dans K possèdent des diviseurs irréductibles unitaires dans $K[X]$

C'est à dire : $\forall A \in K[X] - K : \exists P \in K[X]$ irréductible tq : $P|A$.

Démonstration :

Soit A un polynôme non constant à coefficients dans K et soit E l'ensemble des diviseurs unitaires non constants de A .

Le polynôme unitaire A_0 associé à A est un élément de E (car A_0 est un diviseur unitaire non constants de A). Donc l'ensemble est non vide.

Soit d l'application de E vers $\mathbb{N}^*$ défini par : $d : E \rightarrow \mathbb{N}^*$

$$M \mapsto d(M) = d^0 M.$$

$E \neq \emptyset \Rightarrow d(E) \neq \emptyset$. Soit m le plus petit élément de $d(E)$ et P un élément de E tel que $d^0 P = d(P) = m$.

Montrons que P est un diviseur irréductible unitaire de A dans $K[X]$

Puisque $P \in E$ alors P est un diviseur unitaire de A dans $K[X]$. Il reste à montrer que A est irréductible dans $K[X]$ On a déjà $d^0 P \geq 1$.

Soit Q un diviseur quelconque non constant de A dans $K[X]$ et soit Q_0 le polynôme unitaire associé à A .

$$\left\{ \begin{array}{l} [Q_0|Q \text{ et } Q|A] \Rightarrow Q_0|A \\ Q_0 \text{ est unitaire} \\ d^0 Q_0 = d^0 Q \geq 1 \end{array} \right. \Rightarrow Q_0 \in E \Rightarrow d^0 Q_0 \geq m \Rightarrow d^0 Q = d^0 Q_0 \geq m = d^0 P.$$

$$\left\{ \begin{array}{l} Q|A \\ d^0 Q \geq d^0 P \end{array} \right. \Rightarrow Q \sim A.$$

Donc P est un polynôme irréductible dans $K[X]$.

Ce qui montre que P est un diviseur irréductible unitaire de A dans $K[X]$

Théorème 4-5-4 (de d'Alembert) :

Les polynômes irréductibles à coefficients complexes sont les polynômes de degré 1.

Corollaire 4-5-5 :

Tous les polynômes non constants à coefficients complexes possèdent des racines complexes. C'est à dire : $\forall A \in \mathbb{C}[X] : d^0 A \geq 1 \Rightarrow \exists \alpha \in \mathbb{C} \text{ tq : } A(\alpha) = 0$.

Démonstration :

Soit A un polynôme non constant à coefficients complexes.

D'après le théorème 4-5-3, le polynôme A possède un diviseur irréductible unitaire P à coefficients complexes. D'après le théorème de d'Alembert, $d^0 P = 1$, par suite il existe un nombre complexe a tel que $P = X - a$.

Puisque $X - a = P$ est un diviseur de A alors $A(a) = 0$.

Donc a est une racine complexe de A .

Corollaire 4-5-6 :

Les polynômes irréductibles à coefficients réels sont les polynômes de degré 1 et les polynômes de degré 2 de la forme $aX^2 + bX + c$ tel que, $\Delta = b^2 - 4ac < 0$.

Démonstration :

Soit P un polynôme irréductible à coefficients réels.

$\Rightarrow$) **Si P est irréductible dans $\mathbb{R}[X]$:**

Alors (d'après le corollaire 4-5-5) P admet une racine complexe α (car $d^0P \geq 1$).

- **Si $\alpha \in \mathbb{R}$:**

$$\text{Alors : } \begin{cases} X - \alpha \in \mathbb{R}[X] \\ d^0(X - \alpha) = 1 \geq 1 \Rightarrow P \sim (X - \alpha) \text{ (car } P \text{ est irréductible dans } \mathbb{R}[X]). \\ (X - \alpha) | P \end{cases}$$

Donc : $d^0P = 1$.

- **Si $\alpha \notin \mathbb{R}$:**

Alors α et $\bar{\alpha}$ sont deux racines complexes distincts de P . Donc $(X - \alpha)(X - \bar{\alpha})$ est un diviseur de P .

$(X - \alpha)(X - \bar{\alpha}) = X^2 - (\alpha + \bar{\alpha})X + \alpha\bar{\alpha} = X^2 - 2\text{Re}(\alpha)X + |\alpha|^2 \in \mathbb{R}[X]$. Par suite on a :

$$\begin{cases} X^2 - 2\text{Re}(\alpha)X + |\alpha|^2 \in \mathbb{R}[X] \\ d^0(X^2 - 2\text{Re}(\alpha)X + |\alpha|^2) = 2 \geq 1 \Rightarrow P \sim (X^2 - 2\text{Re}(\alpha)X + |\alpha|^2). \\ (X^2 - 2\text{Re}(\alpha)X + |\alpha|^2) | P \end{cases}$$

Donc il existe un nombre réel non nul a tel que : $P = a(X^2 - 2\text{Re}(\alpha)X + |\alpha|^2)$.

Par conséquent on a : $P = aX^2 - 2a\text{Re}(\alpha)X + a|\alpha|^2$.

Posons : $b = -2a\text{Re}(\alpha)$ et $c = a|\alpha|^2$, alors : $P = aX^2 + bX + c$.

$\Delta = b^2 - 4ac = [-2a\text{Re}(\alpha)]^2 - 4a(a|\alpha|^2) = 4a^2[\text{Re}(\alpha)^2 - |\alpha|^2]$.

Posons : $u = \text{Re}(\alpha)$ et $v = \text{Im}(\alpha)$ alors :

$\Delta = 4a^2[\text{Re}(\alpha)^2 - |\alpha|^2] = 4a^2[u^2 - (u^2 + v^2)] = 4a^2(-v^2) = -4a^2v^2 < 0$.

Ce qui montre que :

P est de degré 2 de la forme $aX^2 + bX + c$ tel que, $\Delta = b^2 - 4ac < 0$.

$\Leftarrow$) - **Si $d^0P = 1$:**

Alors P est irréductible dans $\mathbb{R}[X]$.

- **Si P est de degré 2 de la forme $aX^2 + bX + c$ tel que, $\Delta = b^2 - 4ac < 0$:**

Soit P_0 un diviseur irréductible de P dans $\mathbb{R}[X]$.

$$\begin{cases} P_0 | P \\ P \neq 0 \end{cases} \Rightarrow d^0(P_0) \leq d^0P = 2$$

Soit α une racine complexe de P_0 .

α est aussi une racine de P (car P_0 est un diviseur de P).

Donc $\alpha \notin \mathbb{R}$ (car $\Delta = b^2 - 4ac < 0$) et par suite α et $\bar{\alpha}$ sont deux racines complexes distincts de P_0 . Alors $(X - \alpha)(X - \bar{\alpha})$ est un diviseur de P_0 et par suite $d^0(P_0) \geq 2$.

Par suite $d^0(P_0) = 2 = d^0P$.

$$\begin{cases} P_0 | P \\ d^0(P_0) = d^0P \end{cases} \Rightarrow P \sim P_0.$$

Ce qui montre que P est irréductible dans $\mathbb{R}[X]$.

Exemple 4-5-7 :

- ★ $2X + 1$ est un polynôme irréductible .
- ★ $X^2 + 1$ est un polynôme irréductible dans $\mathbb{R}[X]$.
- ★ $X^2 + 1$ n'est pas un polynôme irréductible dans $\mathbb{C}[X]$.
- ★ $X^4 + 1$ n'est pas un polynôme irréductible.

4-6-Ordre de multiplicité :**Théorème et définition 4-6-1 :**

Soient A et P deux polynômes à coefficients dans K .

Si $A \neq 0$ et si $d^0 P \geq 1$, il existe un entier naturel et un seul appelé l'ordre de multiplicité

de P dans A ou l'ordre de P dans A tel que : $\begin{cases} P^n | A \\ P^{n+1} \nmid A \end{cases}$.

Dans ce cas :

- ★ $P | A \Leftrightarrow n \geq 1$ et dans ce cas on dit aussi que P est un diviseur de A d'ordre de multiplicité n ou P est un diviseur de A d'ordre n .

- ★ Si $n = 1$ (c'est à dire si $\begin{cases} P | A \\ P^2 \nmid A \end{cases}$), on dit aussi que P est un diviseur simple de A .

- ★ Si $n \geq 2$ (c'est dire si $P^2 | A$), on dit aussi que P est un diviseur multiple de A .

Démonstration :**- Existence :**

Supposons que $A \neq 0$ et $d^0 P \geq 1$ et posons $I = \{k \in \mathbb{N} \text{ tq : } P^k | A\}$.

$1 | A \Rightarrow P^0 | A \Rightarrow 0 \in I \Rightarrow I \neq \emptyset$.

$\forall k \in I : k \leq k(d^0 P) = d^0(P^k) \leq d^0 A$ (car $P^k | A$ et $A \neq 0$).

Donc I est une partie non vide de $\mathbb{N}$ majorée par $d^0 A$.

Soit n le plus grand élément de I . Par suite :

$$\begin{cases} n \in I \\ n+1 \notin I \end{cases} \Rightarrow \begin{cases} P^n | A \\ P^{n+1} \nmid A \end{cases} .$$

- Unicité :

Soit m un entier naturel quelconque tel que : $P^m | A$ et $P^{m+1} | A$.

$P^m | A \Rightarrow m \in I \Rightarrow m \leq n$.

Supposons que $m < n$. Alors : $m+1 \leq n \Rightarrow P^{m+1} | P^n$.

$$\begin{cases} P^{m+1} | P^n \\ P^n | A \end{cases} \Rightarrow P^{m+1} | A \text{ ce qui est absurde. Donc } m = n.$$

D'où l'unicité.

Dans ce cas :

- ★ $P | A \Leftrightarrow P^1 | A \Leftrightarrow 1 \in I \Leftrightarrow n \geq 1$

Dans ce cas on dit aussi que P est un diviseur de A d'ordre de multiplicité n ou P est un diviseur de A d'ordre n .

★ Si $n = 1$, c'est dire si $\begin{cases} P|A \\ P^2 \nmid A \end{cases}$ on dit aussi que P est un diviseur simple de A .

★ $\Rightarrow$) Si $n \geq 2$:

$$\text{Alors : } \begin{cases} P^2|P^n \\ P^n|A \end{cases} \Rightarrow P^2|A.$$

$\Leftarrow$) Si $P^2|A$:

Alors : $2 \in I \Rightarrow n \geq 2$.

Donc $n \geq 2$ si seulement si $P^2|A$ et dans ce cas P est un diviseur multiple de A .

Remarque 4-6-2 :

Soient A un polynôme non nul à coefficients dans K et P un polynôme non constant à coefficients dans K d'ordre de multiplicité n dans A .

1) Pour entier naturel k , P^k est un diviseur de A si seulement si $k \leq n$.

C'est à dire : $\forall k \in \mathbb{N} : P^k|A \Leftrightarrow k \leq n$.

2) Si $A, P \in \mathbb{C}[X]$ alors $\overline{P}$ est d'ordre de multiplicité n dans $\overline{A}$.

3) Si $A \in \mathbb{R}[X]$ et si $P \in \mathbb{C}[X]$ alors $\overline{P}$ est d'ordre de multiplicité n dans A .

Démonstration :

1) Soit k un entier naturel quelconque.

$\Rightarrow$) Si P^k est un diviseur de A :

Supposons que $k > n$. Alors : $n + 1 \leq k$, par suite on a :

$$\begin{cases} P^{n+1}|P^k \\ P^k|A \end{cases} \Rightarrow P^{n+1}|A. \text{ Ce qui est absurde.}$$

Donc : $k \leq n$.

$\Leftarrow$) Si $k \leq n$:

$$\text{Alors : } \begin{cases} P^k|P^n \\ P^n|A \end{cases} \Rightarrow P^k|A.$$

2) Supposons que $A, P \in \mathbb{C}[X]$.

$$\begin{cases} P^n|A \\ P^{n+1} \nmid A \end{cases} \Rightarrow \begin{cases} \overline{P}^n|\overline{A} \\ \overline{P}^{n+1} \nmid \overline{A} \end{cases} \Rightarrow \begin{cases} (\overline{P})^n|\overline{A} \\ (\overline{P})^{n+1} \nmid \overline{A} \end{cases}.$$

Donc $\overline{P}$ est d'ordre de multiplicité n dans $\overline{A}$.

3) Supposons que $A \in \mathbb{R}[X]$ et $P \in \mathbb{C}[X]$.

$\overline{P}$ est d'ordre de multiplicité n dans $\overline{A} = A$ dans le cas où $A \in \mathbb{R}[X]$ est un polynôme à coefficients réels.

Proposition 4-6-3 :

Soient A un polynôme non nul à coefficients dans K , P un polynôme non constant à coefficients dans K et n un entier naturel.

P est d'ordre de multiplicité n dans A si seulement s'il existe un polynôme $A_0 \in K[X]$

tel que : $\begin{cases} A = P^n A_0 \\ P \nmid A_0 \end{cases}$. C'est à dire :

$$[P \text{ est d'ordre de multiplicité } n] \Leftrightarrow \exists A_0 \in K[X] \quad tq : \begin{cases} A = P^n A_0 \\ P \nmid A_0 \end{cases}.$$

Dans ce cas A_0 est le quotient de la division euclidienne de A par P^n .

Démonstration :

$\Rightarrow$) **Si P est d'ordre de multiplicité n dans A :**

$$P^n | A \Rightarrow \exists A_0 \in K[X] \quad tq : A = P^n A_0.$$

Supposons que P est un diviseur de A_0 .

$$\text{Alors : } \exists Q \in K[X] \quad tq : A_0 = PQ \text{ et par suite : } A = P^n PQ = P^{n+1}Q \Rightarrow P^{n+1} | A.$$

Ce qui est absurde.

$$\text{Alors : } \begin{cases} A = P^n A_0 \\ P \nmid A_0 \end{cases}.$$

$\Leftarrow$) **S'il existe un polynôme $A_0 \in K[X]$ tel que $A = P^n A_0$ et $P \nmid A_0$:**

$$A = P^n A_0 \Rightarrow P^n | A.$$

Supposons que P^{n+1} est un diviseur de A .

$$\text{Alors : } \exists Q \in K[X] \quad tq : A = P^{n+1}Q.$$

$$\text{Donc : } P^n A_0 = A = P^{n+1}Q \Rightarrow A_0 = PQ \Rightarrow P | A_0. \text{ Ce qui est absurde.}$$

$$\text{Par conséquent } \begin{cases} A = P^n A_0 \\ P \nmid A_0 \end{cases}.$$

Ce qui montre que P est d'ordre de multiplicité n dans A .

Dans ce cas A_0 est le quotient de la division euclidienne de A par P^n .

Corollaire 4-6-4 :

Soient A un polynôme non nul à coefficients dans K ; P un polynôme non constant à coefficients dans K d'ordre de multiplicité n dans A , A_0 est le quotient de la division euclidienne de A par P^n et Q un polynôme non constant à coefficients dans K premier à P

L'ordre de multiplicité de Q dans A est égal à l'ordre de multiplicité de Q dans A_0 .

Démonstration :

Puisque n est l'ordre de multiplicité de P dans A et puisque A_0 est le quotient de la

$$\text{division euclidienne de } A \text{ par } P^n \text{ alors on a : } \begin{cases} A = P^n A_0 \\ P \nmid A_0 \end{cases}.$$

Soit m l'ordre de multiplicité de Q dans A_0 et soit A_1 le quotient de la division euclidienne

$$\text{de } A_0 \text{ par } Q^m \text{ alors on a : } \begin{cases} A_0 = Q^m A_1 \\ Q \nmid A_1 \end{cases}.$$

$$\text{Par suite : } A = P^n Q^m A_1 = Q^m P^n A_1 = Q^m (P^n A_1).$$

Supposons que Q est un diviseur de $P^n A_1$. Alors :

$$\begin{cases} Q \neq 0 \\ Q \wedge P = 1 \\ Q | (P^n A_1) \end{cases} \Rightarrow \begin{cases} Q \neq 0 \\ Q \wedge P^n = 1 \\ Q | (P^n A_1) \end{cases} \Rightarrow Q | A_1. \text{ Ce qui est absurde.}$$

Donc Q n'est pas un diviseur de $P^n A_1$. Par conséquent on a :
$$\begin{cases} A = Q^m (P^n A_1) \\ Q \nmid (P^n A_1) \end{cases}.$$

Ce qui montre que l'ordre de multiplicité de Q dans A est égal à l'ordre de multiplicité m de Q dans A_0 .

Définition 4-6-5 :

Soient A un polynôme non nul à coefficients dans K et si $a \in K$, l'ordre de multiplicité du polynôme $X - a$ dans A est appelé aussi l'ordre de multiplicité a dans A .

- ★ Si $X - a$ est un diviseur simple de A on dit aussi que a est une racine simple de A .
- ★ Si $X - a$ est un diviseur multiple de A on dit aussi que a est une racine multiple de A .

Remarque 4-6-6 :

Soient A un polynôme non nul à coefficients dans K , $a \in K$ et n l'ordre de multiplicité de a dans A .

1) a est une racine de A si seulement si $n \geq 1$.

Dans ce cas on dit aussi que " a est une racine de A d'ordre de multiplicité n " ou " a est une racine de A d'ordre n ".

2) Si $A \in \mathbb{C}[X]$ alors n est l'ordre de multiplicité de $\bar{a}$ dans $\bar{A}$.

3) Si $A \in \mathbb{R}[X]$ alors n est l'ordre de multiplicité de $\bar{a}$ dans A .

Démonstration :

1) $[a \text{ est une racine de } A] \Leftrightarrow (X - a) | A \Leftrightarrow n \geq 1$.

2) Supposons que $K = \mathbb{C}$ et que $a \in \mathbb{C}$.

$$\begin{aligned} [a \text{ est d'ordre de multiplicité } n \text{ dans } A] &\Rightarrow [X - a \text{ est d'ordre de multiplicité } n \text{ dans } A] \\ &\Rightarrow [\overline{X - a} \text{ est d'ordre de multiplicité } n \text{ dans } \bar{A}] \\ &\Rightarrow [X - \bar{a} \text{ est d'ordre de multiplicité } n \text{ dans } \bar{A}] \\ &\Rightarrow [\bar{a} \text{ est d'ordre de multiplicité } n \text{ dans } \bar{A}]. \end{aligned}$$

3) Supposons que $K = \mathbb{R}$ et que $a \in \mathbb{C}$.

$$[a \text{ est d'ordre de multiplicité } n \text{ dans } A] \Rightarrow [\bar{a} \text{ est d'ordre de multiplicité } n \text{ dans } \bar{A} = A].$$

Corollaire 4-6-7 :

Soient A un polynôme non nul à coefficients dans K , a un élément de K et n un entier naturel a est d'ordre de multiplicité n dans A si seulement s'il existe un polynôme

$$A_0 \in K[X] \text{ tel que : } \begin{cases} A = (X - a)^n A_0 \\ a \text{ n'est pas une racine de } A_0 \end{cases}. \text{ C'est à dire :}$$

$$[a \text{ est d'ordre de multiplicité } n \text{ dans } A]$$

$$\Leftrightarrow \exists A_0 \in K[X] \text{ tq : } \begin{cases} A = (X - a)^n A_0 \\ a \text{ n'est pas une racine de } A_0 \end{cases}.$$

Dans ce cas : A_0 est le quotient de la division euclidienne de A par $(X - a)^n$.

Démonstration :

$[a \text{ est d'ordre de multiplicité } n \text{ dans } A]$

$$\Leftrightarrow [X - a \text{ est d'ordre de multiplicité } n \text{ dans } A]$$

$$\Leftrightarrow \exists A_0 \in K[X] \quad tq : \begin{cases} A = (X - a)^n A_0 \\ (X - a) \nmid A_0 \end{cases}$$

$$\Leftrightarrow \exists A_0 \in K[X] \quad tq : \begin{cases} A = (X - a)^n A_0 \\ a \text{ n'est pas une racine de } A_0 \end{cases} .$$

Dans ce cas : A_0 est le quotient de la division euclidienne de A par $(X - a)^n$.

Corollaire 4-6-8 :

Soient A un polynôme non nul à coefficients dans K , $a, b \in K$ distincts, n l'ordre de multiplicité de a dans A et A_0 le quotient de la division euclidienne de A par $(X - a)^n$.

L'ordre de multiplicité de b dans A est égal à l'ordre de multiplicité de b dans A_0 .

Démonstration :

Soient m l'ordre de multiplicité de b dans A_0 .

Alors n est l'ordre de multiplicité de $X - a$ dans A et m est l'ordre de multiplicité de $X - b$ dans A_0 .

$$a \neq b \Rightarrow (X - a) \wedge (X - b) = 1.$$

D'après le corollaire 4-6-4, m est l'ordre de multiplicité de $X - b$ dans A .

Donc l'ordre de multiplicité de b dans A est égal à l'ordre de multiplicité m de b dans A_0 .

Exemple 4-6-9 :

Dans $\mathbb{R}[X]$ soit $A = 2X^8 + 5X^7 + 7X^6 + 9X^5 + 7X^4 + 3X^3 + X^2 - X - 1$.

On peut utiliser le procédé de Hôrner pour déterminer les ordres de multiplicité des racines de A .

	2	5	7	9	7	3	1	-1	-1
-1		-2	-3	-4	-5	-2	-1	0	1
	2	3	4	5	2	1	0	-1	0
-1		-2	-1	-3	-2	0	-1	1	
	2	1	3	2	0	1	-1	0	
-1		-2	1	-4	2	-2	1		
	2	-1	4	-2	2	-1	0		
-1		-2	3	-7	9	-11			
	2	-3	7	-9	11	-12			

Donc -1 est une racine de A d'ordre de multiplicité 3 et

$A_1 = 2X^5 - X^4 + 4X^3 - 2X^2 + 2X - 1$ est le quotient de la division euclidienne de A par $(X + 1)^3$.

	2	-1	4	-2	2	-1
$\frac{1}{2}$		1	0	2	0	1
	2	0	4	0	2	0
$\frac{1}{2}$		1	$\frac{1}{2}$	$\frac{9}{4}$	$\frac{9}{8}$	
	2	1	$\frac{9}{2}$	$\frac{9}{4}$	$\frac{25}{8}$	

Donc $\frac{1}{2}$ est une racine simple de A et $A_2 = 2X^4 + 4X^2 + 2$ est le quotient de la division euclidienne de A_1 par $X - \frac{1}{2}$.

	2	0	4	0	2
i		$2i$	-2	$2i$	-2
	2	$2i$	2	$2i$	0
i		$2i$	-4	$-2i$	
	2	$4i$	-2	0	
i		$2i$	-6		
	2	$6i$	-8		

Donc i est une racine de A d'ordre de multiplicité 2 et $A_3 = 2X^2 + 4iX - 2$ est le quotient de la division euclidienne de A_2 par $(X - i)^2$.

$$A_3 = 2X^2 + 4iX - 2 = A_3 = 2(X^2 + 2iX - 1) = 2(X + i)^2.$$

Donc $-i$ est une racine de A d'ordre de multiplicité 2.

Lemme 4-6-10 :

Soient A et P deux polynômes à coefficients dans K et n un entier naturel non nul.

Si P^n est un diviseur de A alors P^{n-1} est un diviseur de A' . C'est à dire :

$$P^n | A \Rightarrow P^{n-1} | A'.$$

Démonstration :

Supposons que P^n est un diviseur de A .

Il existe alors un polynôme Q à coefficients dans K tel que $A = P^n Q$.

$$A' = (P^n)' Q + P^n Q' = nP^{n-1} P' Q + P^n Q' = P^{n-1} (nP' Q + P Q').$$

Donc P^{n-1} est un diviseur de A' .

Lemme 4-6-11 :

Soient A et P deux polynômes à coefficients dans K et n un entier naturel non nul.

Si P^n est un diviseur de A alors pour tout entier naturel $k = 0, 1, \dots, n-1$, P^{n-k} est un diviseur de $A^{(k)}$. C'est à dire : $\forall k = 0, 1, \dots, n-1 : P^{n-k} | A^{(k)}$.

Démonstration :

Supposons que P^n est un diviseur de A .

Posons $I = \{k = 0, 1, \dots, n-1 \mid P^{n-k} \nmid A^{(k)}\}$ et supposons que $I \neq \emptyset$.

Puisque I est une partie non vide de $\mathbb{N}$ alors I admet un plus petit élément r .

$P^n | A \Rightarrow P^{n-0} | A^{(0)} \Rightarrow 0 \notin I \Rightarrow r \neq 0 \Rightarrow r \geq 1 \Rightarrow r-1 \in \{0, 1, \dots, n-2\}$.

Puisque r est le plus petit élément de I alors $r-1 \notin I$.

$$\begin{cases} r-1 \notin I \\ r-1 \in \{0, 1, \dots, n-2\} \end{cases} \Rightarrow P^{n-(r-1)} | A^{(r-1)} \Rightarrow P^{n-r+1} | A^{(r-1)}.$$

Donc : $P^{n-r+1-1} | [A^{(r-1)}]' \Rightarrow P^{n-r} | A^{(r)} \Rightarrow r \notin I$ ce qui est absurde.

Donc : $I = \emptyset$.

Ce qui montre que : $\forall k = 0, 1, \dots, n-1 : P^{n-k} | A^{(k)}$.

Lemme 4-6-12 :

Soient A et P deux polynômes à coefficients dans K et n un entier naturel non nul.

Si P^n est un diviseur de A alors : $\forall k = 0, 1, \dots, n-1 : P | A^{(k)}$.

C'est à dire : $P^n | A \Rightarrow \forall k = 0, 1, \dots, n-1 : P | A^{(k)}$.

Démonstration :

Supposons que P^n est un diviseur de A .

$\forall k = 0, 1, \dots, n-1 : n-k \geq 1 \Rightarrow P | P^{n-k}$

$$\begin{cases} P | P^{n-k} \\ P^{n-k} | A^{(k)} \end{cases} \Rightarrow \forall k = 0, 1, \dots, n-1 : P | A^{(k)}.$$

Théorème 4-6-13 :

Soient A un polynôme à coefficients dans K , a un élément de K et n un entier naturel non nul.

Si $(X-a)^n$ est un diviseur de A alors : $A(a) = A'(a) = \dots = A^{(n-1)}(a) = 0$.

C'est à dire : $(X-a)^n | A \Rightarrow A(a) = A'(a) = \dots = A^{(n-1)}(a) = 0$.

Démonstration :

Supposons que $(X-a)^n$ est un diviseur de A .

$(X-a)^n | A \Rightarrow \forall k = 0, 1, \dots, n-1 : (X-a) | A^{(k)}$

$\Rightarrow A(a) = A'(a) = \dots = A^{(n-1)}(a) = 0$.

Théorème 4-6-14 :

Soient A un polynôme à coefficients dans K , a un élément de K et n un entier naturel non nul.

Si K est de caractéristique 0 alors $(X-a)^n$ est un diviseur de A si et seulement si :

$$A(a) = A'(a) = \dots = A^{(n-1)}(a) = 0.$$

C'est à dire si $\text{cara}(K) = 0$ alors :

$$(X-a)^n | A \Leftrightarrow A(a) = A'(a) = \dots = A^{(n-1)}(a) = 0.$$

Démonstration :

$\Rightarrow$) Si $(X - a)^n$ est un diviseur de A :

Alors (d'après le théorème 4-6-13) on a : $A(a) = A'(a) = \dots = A^{(n-1)}(a) = 0$.

$\Leftarrow$) Si $A(a) = A'(a) = \dots = A^{(n-1)}(a) = 0$:

Posons : $m = \max(n, d^0(A))$.

D'après la formule de Taylor appliquée à A et a on a : $A = \sum_{k=0}^m \frac{A^{(k)}(a)}{k!} (X - a)^k$.

Puisqu'on a : $A(a) = A'(a) = \dots = A^{(n-1)}(a) = 0$ alors :

$$A = \sum_{k=n}^m \frac{A^{(k)}(a)}{k!} (X - a)^k.$$

$$\text{Donc : } A = (X - a)^n \left[\sum_{k=n}^m \frac{A^{(k)}(a)}{k!} (X - a)^{k-n} \right] \Rightarrow (X - a)^n | A.$$

Corollaire 4-6-15 :

Soient A un polynôme non nul à coefficients dans K et a un élément de K .

Si K est de caractéristique 0 alors a est une racine multiple de A si et seulement si

$$A(a) = A'(a) = 0$$

C'est à dire si K est de caractéristique 0 alors :

$$a \text{ est une racine multiple de } A \Leftrightarrow A(a) = A'(a) = 0.$$

Démonstration :

Supposons que K est de caractéristique 0.

$$[a \text{ est une racine multiple de } A] \Leftrightarrow [X - a \text{ est un diviseur multiple de } A]$$

$$\Leftrightarrow (X - a)^2 | A$$

$$\Leftrightarrow A(a) = A'(a) = 0.$$

Corollaire 4-6-16 :

Soient A un polynôme non nul à coefficients dans K , a un élément de K et n un entier naturel non nul.

Si K est de caractéristique 0 alors a est une racine de A d'ordre de multiplicité n si et seulement si :

$$\begin{cases} A(a) = A'(a) = \dots = A^{(n-1)}(a) = 0 \\ A^{(n)}(a) \neq 0 \end{cases}.$$

C'est à dire :

$$a \text{ est une racine de } A \text{ d'ordre } n \Leftrightarrow \begin{cases} A(a) = A'(a) = \dots = A^{(n-1)}(a) = 0 \\ A^{(n)}(a) \neq 0 \end{cases}.$$

Démonstration :

Supposons que K est de caractéristique 0.

$$[a \text{ est une racine de } A \text{ d'ordre de multiplicité } n]$$

$$\Leftrightarrow [X - a \text{ est un diviseur de } A \text{ d'ordre de multiplicité } n]$$

$$\Leftrightarrow \begin{cases} (X-a)^n | A \\ (X-a)^{n+1} \nmid A \end{cases}$$

$$\Leftrightarrow \begin{cases} A(a) = A'(a) = \dots = A^{(n-1)}(a) = 0 \\ A^{(n)}(a) \neq 0 \end{cases}.$$

Exemple 4-6-17 :

Dans $\mathbb{R}$ soit $A = 2X^8 + 5X^7 + 7X^6 + 9X^5 + 7X^4 + 3X^3 + X^2 - X - 1$.

$$A(-1) = 2 - 5 + 7 - 9 + 7 - 3 + 1 + 1 - 1 = 0$$

$$\begin{aligned} A\left(\frac{1}{2}\right) &= \frac{2}{2^8} + \frac{5}{2^7} + \frac{7}{2^6} + \frac{9}{2^5} + \frac{7}{2^4} + \frac{3}{2^3} + \frac{1}{2^2} - \frac{1}{2} - 1 \\ &= \frac{1}{2^7} + \frac{5}{2^7} + \frac{7}{2^6} + \frac{9}{2^5} + \frac{7}{2^4} + \frac{3}{2^3} + \frac{1}{2^2} - \frac{3}{2} \\ &= \frac{1 + 5 + 14 + 9 \times 2^2 + 7 \times 2^3 + 3 \times 2^4 + 2^5 - 3 \times 2^6}{2^7} \\ &= \frac{20 + 9 \times 4 + 7 \times 8 + 3 \times 16 + 32 - 3 \times 64}{2^7} \\ &= \frac{20 + 36 + 56 + 48 + 32 - 192}{2^7} = 0 \end{aligned}$$

$$\begin{aligned} A(i) &= 2i^8 + 5i^7 + 7i^6 + 9i^5 + 7i^4 + 3i^3 + i^2 - i - 1 \\ &= 2 - 5i - 7 + 9i + 7 - 3i - 1 - i - 1 = 0 \end{aligned}$$

$$\begin{aligned} A(-i) &= 2(-i)^8 + 5(-i)^7 + 7(-i)^6 + 9(-i)^5 + 7(-i)^4 + 3(-i)^3 + (-i)^2 + i - 1 \\ &= 2 + 5i - 7 - 9i + 7 + 3i - 1 + i - 1 = 0 \end{aligned}$$

Donc $-1, \frac{1}{2}, i, -i$ sont des racines de A .

$$A' = 16X^7 + 35X^6 + 42X^5 + 45X^4 + 28X^3 + 9X^2 + 2X - 1.$$

$$A'(-1) = -16 + 35 - 42 + 45 - 28 + 9 - 2 - 1 = 0$$

$$\begin{aligned} A'\left(\frac{1}{2}\right) &= \frac{16}{2^7} + \frac{35}{2^6} + \frac{42}{2^5} + \frac{45}{2^4} + \frac{28}{2^3} + \frac{9}{2^2} + 1 - 1 \\ &= \frac{8}{2^6} + \frac{35}{2^6} + \frac{42}{2^5} + \frac{45}{2^4} + \frac{28}{2^3} + \frac{9}{2^2} > 0. \text{ Alors : } A'\left(\frac{1}{2}\right) \neq 0 \end{aligned}$$

Donc $\frac{1}{2}$ est une racine simple de A .

$$\begin{aligned} A'(i) &= 16i^7 + 35i^6 + 42i^5 + 45i^4 + 28i^3 + 9i^2 + 2i - 1 \\ &= -16i - 35 + 42i + 45 - 28i - 9 + 2i - 1 = 0. \end{aligned}$$

$$\begin{aligned} A'(-i) &= 16(-i)^7 + 35(-i)^6 + 42(-i)^5 + 45(-i)^4 + 28(-i)^3 + 9(-i)^2 - 2i - 1 \\ &= 16i - 35 - 42i + 45 + 28i - 9 - 2i - 1 = 0. \end{aligned}$$

$$A'' = 112X^6 + 210X^5 + 210X^4 + 180X^3 + 84X^2 + 18X + 2.$$

$$A''(-1) = 112 - 210 + 210 - 180 + 84 - 18 + 2 = 0.$$

$$\begin{aligned} A''(i) &= 112i^6 + 210i^5 + 210i^4 + 180i^3 + 84i^2 + 18i + 2 \\ &= -112 + 210i + 210 - 180i - 84 + 18i + 2 = 16 + 48i \neq 0. \end{aligned}$$

Donc i est une racine de A d'ordre de multiplicité 2.

$$\begin{aligned} A''(-i) &= 112(-i)^6 + 210(-i)^5 + 210(-i)^4 + 180(-i)^3 + 84(-i)^2 - 18i + 2 \\ &= -112 - 210i + 210 + 180i - 84 - 18i + 2 = 16 - 48i \neq 0. \end{aligned}$$

Donc $-i$ est une racine de A d'ordre de multiplicité 2.

$$A''' = 672X^5 + 1050X^4 + 840X^3 + 540X^2 + 168X + 18.$$

$$A'''(-1) = -672 + 1050 - 840 + 540 - 168 + 18 = -72 \neq 0.$$

Donc -1 est une racine de A d'ordre de multiplicité 3.

4-7-Factorisation :

Théorème 4-7-1 :

Soient A un polynôme à coefficients dans K , $P_1, P_2, \dots, P_n$ des polynômes irréductibles dans $K[X]$ non associés deux à deux, $\alpha_1, \alpha_2, \dots, \alpha_n$ des entiers naturels et a un élément non nul de K .

Si $A = aP_1^{\alpha_1}P_2^{\alpha_2}\dots P_n^{\alpha_n}$ alors A est non nul et $\alpha_1, \alpha_2, \dots, \alpha_n$ sont les ordres de multiplicité respectivement de $P_1, P_2, \dots, P_n$ dans A .

Démonstration :

Supposons que $A = aP_1^{\alpha_1}P_2^{\alpha_2}\dots P_n^{\alpha_n}$. $A \neq 0$ car $a, P_1, P_2, \dots, P_n$ sont non nuls.

- Si $n = 1$:

Alors : $A = aP_1^{\alpha_1} \Rightarrow \begin{cases} A = aP_1^{\alpha_1} \\ P_1 \nmid a \end{cases}$. Donc α_1 est l'ordre de multiplicité de P_1 dans A .

- Si $n \geq 2$:

$\forall k = 1, 2, \dots, n$: posons : $A_0 = a \prod_{i=1, i \neq k}^n P_i^{\alpha_i}$ alors :

$$\star A = A_0 P_k^{\alpha_k}.$$

$$\star [\forall i \in \{1, \dots, n\} - \{k\} : P_k \nmid P_i = 1] \Rightarrow P_k \nmid A_0 = 1 \Rightarrow P_k \nmid A_0.$$

Donc α_k est l'ordre de multiplicité de P_k dans A .

Ce qui montre que $\alpha_1, \alpha_2, \dots, \alpha_n$ sont les ordres de multiplicité respectivement de $P_1, P_2, \dots, P_n$ dans A .

Théorème 4-7-2 :

Soient A un polynôme à coefficients dans K , $P_1, P_2, \dots, P_n$ des polynômes irréductibles dans $K[X]$ non associés deux à deux, $\alpha_1, \alpha_2, \dots, \alpha_n$ des entiers naturels et a un élément non nul de K .

Si $A = aP_1^{\alpha_1}P_2^{\alpha_2}\dots P_n^{\alpha_n}$ alors pour tout diviseur B de A dans $K[X]$ il existe un élément non

b de K et des entiers naturels $\beta_1, \beta_2, \dots, \beta_n$ tels que :
$$\begin{cases} B = bP_1^{\beta_1}P_2^{\beta_2}\dots P_n^{\beta_n} \\ \forall k = 1, 2, \dots, n : \beta_k \leq \alpha_k \end{cases}$$

Démonstration :

Supposons que $A = aP_1^{\alpha_1}P_2^{\alpha_2}\dots P_n^{\alpha_n}$ et soit B un diviseur quelconque de A .

D'après le théorème 4-7-1, A est non nul et $\alpha_1, \alpha_2, \dots, \alpha_n$ sont les ordres de multiplicité respectivement de $P_1, P_2, \dots, P_n$ dans A .

Pour tout entier naturel $k = 1, 2, \dots, n$: posons β_k l'ordre de multiplicité de P_k dans B .

$$\forall k = 1, 2, \dots, n : \begin{cases} P_k^{\beta_k} \mid B \\ B \mid A \end{cases} \Rightarrow P_k^{\beta_k} \mid A \Rightarrow \beta_k \leq \alpha_k.$$

$P_1^{\beta_1} P_2^{\beta_2} \dots P_n^{\beta_n}$ est un diviseur de B dans $K[X]$.

Alors il existe un polynôme $Q \in K[X]$ tel que $B = P_1^{\beta_1} P_2^{\beta_2} \dots P_n^{\beta_n} Q$.

Supposons que $d^0 Q \geq 1$ et soit P un diviseur irréductible unitaire de Q dans $K[X]$.

$[P|Q \text{ et } Q|B \text{ et } B|A] \Rightarrow P|A \Rightarrow \exists k = 1, 2, \dots, n \text{ tq : } P = P_k$.

$P_k|Q \Rightarrow \exists S \in K[X] \text{ tq : } Q = P_k S$. Par conséquent $B = P_1^{\beta_1} P_2^{\beta_2} \dots P_n^{\beta_n} P_k S$.

Donc $P_k^{\beta_k+1} = P_k^{\beta_k} P_k$ est un diviseur de B dans $K[X]$.

Ce qui est absurde (car β_k est l'ordre de multiplicité P_k dans B).

Ce qui prouve que Q est une constante non nulle b dans K .

On a alors :
$$\begin{cases} B = b P_1^{\beta_1} P_2^{\beta_2} \dots P_n^{\beta_n} \\ \forall k = 1, 2, \dots, n : \beta_k \leq \alpha_k \end{cases}$$

Définition 4-7-3 :

Soient A un polynôme à coefficients dans K , $P_1, P_2, \dots, P_n$ des polynômes irréductibles dans $K[X]$ non associés deux à deux, $\alpha_1, \alpha_2, \dots, \alpha_n$ des entiers naturels non nuls et a un élément non nul de K .

Si $A = a P_1^{\alpha_1} P_2^{\alpha_2} \dots P_n^{\alpha_n}$ on dit que $A = a P_1^{\alpha_1} P_2^{\alpha_2} \dots P_n^{\alpha_n}$ est une décomposition de A en facteurs irréductibles dans $K[X]$ ou $a P_1^{\alpha_1} P_2^{\alpha_2} \dots P_n^{\alpha_n}$ est une factorisation de A dans $K[X]$

La recherche d'une factorisation de A dans $K[X]$ est appelée la décomposition de A en facteurs irréductibles dans $K[X]$ ou la factorisation de A dans $K[X]$.

Si de plus $P_1, P_2, \dots, P_n$ sont unitaires dans $K[X]$ distincts deux à deux et si

$A = a P_1^{\alpha_1} P_2^{\alpha_2} \dots P_n^{\alpha_n}$ on dit que $A = a P_1^{\alpha_1} P_2^{\alpha_2} \dots P_n^{\alpha_n}$ est une décomposition de A en facteurs irréductibles unitaires dans $K[X]$.

Théorème 4-7-4 :

Tout polynôme non constant A (c'est à dire $d^0 A \geq 1$) à coefficients dans K admet une décomposition en facteurs irréductibles unitaires $A = a P_1^{\alpha_1} P_2^{\alpha_2} \dots P_n^{\alpha_n}$ dans $K[X]$ et une seule à un ordre multiplicatif près (c'est à dire si $A = b Q_1^{\beta_1} Q_2^{\beta_2} \dots Q_m^{\beta_m}$ est une autre décomposition en facteurs irréductibles unitaires de A alors $a = b$, $n = m$ et il existe une permutation $\sigma \in S_n$ telle que : $\forall i = 1, 2, \dots, n : Q_i = P_{\sigma(i)}$ et $\beta_i = \alpha_{\sigma(i)}$).

★ a est le coefficient dominant de A .

★ $P_1, P_2, \dots, P_n$ sont les diviseurs irréductibles unitaires de A dans $K[X]$ distincts deux à deux.

★ $\alpha_1, \alpha_2, \dots, \alpha_n$ sont les ordres de multiplicité respectivement de $P_1, P_2, \dots, P_n$ dans A .

Démonstration :

Soient A un polynôme non constant A à coefficients dans K et a son coefficient dominant.

- **Existence :**

Soient $P_1, P_2, \dots, P_n$ les diviseurs irréductibles unitaires de A dans $K[X]$ distincts deux à deux et $\alpha_1, \alpha_2, \dots, \alpha_n$ les ordres de multiplicité de $P_1, P_2, \dots, P_n$ dans A .

Alors $P_1^{\alpha_1} P_2^{\alpha_2} \dots P_n^{\alpha_n}$ est un diviseur de A dans $K[X]$.

Donc il existe un polynôme $Q \in K[X]$ tel que $A = P_1^{\alpha_1} P_2^{\alpha_2} \dots P_n^{\alpha_n} Q$.

Supposons que $d^0 Q \geq 1$ et soit P un diviseur irréductible unitaire de Q dans $K[X]$.

P est aussi un diviseur irréductible unitaire de A dans $K[X]$ (car $Q|A$).

Par suite il existe $k = 1, 2, \dots, n$ tel que : $P = P_k$.

$P_k|Q \Rightarrow \exists S \in K[X] \text{ tq : } Q = P_k S$. Par conséquent $A = P_1^{\alpha_1} P_2^{\alpha_2} \dots P_n^{\alpha_n} P_k S$

Donc $P_k^{\alpha_k+1} = P_k^{\alpha_k} P_k$ est un diviseur de A dans $K[X]$.

Ce qui est absurde (car P_k est un diviseur de A d'ordre de multiplicité α_k).

Ce qui prouve que Q est une constante non nulle.

Puisque $P_1^{\alpha_1} P_2^{\alpha_2} \dots P_n^{\alpha_n}$ est unitaire, $Q \in K^*$ et $A = Q P_1^{\alpha_1} P_2^{\alpha_2} \dots P_n^{\alpha_n}$ alors

$Q = a$ est le coefficient dominant de A et on a donc : $A = a P_1^{\alpha_1} P_2^{\alpha_2} \dots P_n^{\alpha_n}$.

D'où l'existence.

- Unicité :

Soit $A = b Q_1^{\beta_1} Q_2^{\beta_2} \dots Q_m^{\beta_m}$ est une autre décomposition en facteurs irréductibles unitaires de A

D'après le théorème 4-7-1, $\beta_1, \beta_2, \dots, \beta_m$ sont les ordres de multiplicité respectivement de $Q_1, Q_2, \dots, Q_m$ dans A .

Puisque $Q_1^{\beta_1} Q_2^{\beta_2} \dots Q_m^{\beta_m}$ est unitaire alors $b = a$ est le coefficient dominant de A .

$\forall i = 1, 2, \dots, m$:

$$\begin{cases} Q_i|A \\ Q_i \text{ est irréductible unitaire dans } K[X] \end{cases} \Rightarrow \exists k_i = 1, 2, \dots, n : Q_i = P_{k_i}.$$

Posons $I = \{1, 2, \dots, m\}$, $J = \{1, 2, \dots, n\}$ et soit σ l'application de I vers J définie par :

$$\begin{aligned} \sigma : I &\rightarrow J \\ k &\mapsto \sigma(i) = k_i. \end{aligned}$$

Par suite on a : $\forall i \in I : Q_i = P_{k_i} = P_{\sigma(i)}$.

Montrons que σ est une bijection de I vers J .

★ $\forall i, j \in I : \sigma(i) = \sigma(j) \Rightarrow P_{\sigma(i)} = P_{\sigma(j)} \Rightarrow Q_i = Q_j \Rightarrow i = j$.

Donc σ est injective.

★ $\forall j \in J : P_j$ est un diviseur irréductible unitaire de $A = a Q_1^{\beta_1} Q_2^{\beta_2} \dots Q_m^{\beta_m}$

Alors : $\exists i \in I \text{ tq : } P_j = Q_i$. On a donc : $P_j = Q_i = P_{\sigma(i)} \Rightarrow j = \sigma(i)$.

Donc σ est surjective.

Ce qui prouve que σ est une bijection de I vers J .

Par suite $m = |I| = |J| = n$ et $\sigma \in S_n$.

$\forall i \in I$: puisque β_i est l'ordre de multiplicité de $Q_i = P_{\sigma(i)}$ alors $\beta_i = \alpha_{\sigma(i)}$.

$$\text{On a donc : } b = a, m = n, \sigma \in S_n \text{ et } \forall i = 1, 2, \dots, n : \begin{cases} Q_i = P_{\sigma(i)} \\ \beta_i = \alpha_{\sigma(i)} \end{cases}.$$

D'où l'unicité à un multiplicatif ordre près.

Corollaire 4-7-5 :

Pour tout polynôme non constant A (c'est à dire $d^0 A \geq 1$) à coefficients complexes la décomposition en facteurs irréductibles unitaires de A dans $\mathbb{C}[X]$ est

$A = a(X - a_1)^{\alpha_1} (X - a_2)^{\alpha_2} \dots (X - a_n)^{\alpha_n}$ où :

★ a est le coefficient dominant de A .

★ $a_1, a_2, \dots, a_n$ sont les racines distinctes de A dans $\mathbb{C}$.

★ $\alpha_1, \alpha_2, \dots, \alpha_n$ sont les ordres de multiplicité des racines $a_1, a_2, \dots, a_n$ dans A .

Démonstration :

Soient A un polynôme non constant A à coefficients complexes, a son coefficient dominant, $a_1, a_2, \dots, a_n$ les racines distinctes de A dans $\mathbb{C}$ et $\alpha_1, \alpha_2, \dots, \alpha_n$ les ordres multiplicité des racines $a_1, a_2, \dots, a_n$ dans A .

Alors a est le coefficient dominant de A , $X - a_1, X - a_2, \dots, X - a_n$ les diviseurs irréductibles unitaires de A dans $\mathbb{C}[X]$ distincts deux à deux et $\alpha_1, \alpha_2, \dots, \alpha_n$ les ordres de multiplicité de $X - a_1, X - a_2, \dots, X - a_n$ dans A .

Donc $A = a(X - a_1)^{\alpha_1}(X - a_2)^{\alpha_2}, \dots, (X - a_n)^{\alpha_n}$ est la décomposition en facteurs irréductibles unitaires de A dans $\mathbb{C}[X]$

Exemple 4-7-6 :

Soit $A = 2X^8 + 5X^7 + 7X^6 + 9X^5 + 7X^4 + 3X^3 + X^2 - X - 1$.

- 1^{ière} méthode :

On utilise les dérivées successives.

On a vu que -1 est une racine de A d'ordre de multiplicité 3 et que

$\frac{1}{2}$ est une racine simple de A .

Posons $B = (X + 1)^3 \left(X - \frac{1}{2}\right)$ alors :

$$\begin{aligned} B &= (X^3 + 3X^2 + 3X + 1) \left(X - \frac{1}{2}\right) = X^4 + \frac{5}{2}X^3 + \frac{3}{2}X^2 - \frac{1}{2}X - \frac{1}{2} \\ &= \frac{1}{2}(2X^4 + 5X^3 + 3X^2 - X - 1). \end{aligned}$$

Posons $B_0 = 2X^4 + 5X^3 + 3X^2 - X - 1$ alors : $B = \frac{1}{2}B_0 \Rightarrow B_0 = 2B$.

On effectue la division euclidienne de A par B_0 .

$$\begin{array}{r|l} 2X^8 + 5X^7 + 7X^6 + 9X^5 + 7X^4 + 3X^3 + X^2 - X - 1 & 2X^4 + 5X^3 + 3X^2 - X - 1 \\ 0 & A_0 = X^4 + 2X^2 + 1 \end{array}$$

Alors : $A = B_0 A_0 = 2B A_0 = 2(X + 1)^3 \left(X - \frac{1}{2}\right) (X^4 + 2X^2 + 1)$

$$= 2(X + 1)^3 \left(X - \frac{1}{2}\right) (X^2 + 1)^2$$

$$= 2(X + 1)^3 \left(X - \frac{1}{2}\right) (X - i)^2 (X + i)^2.$$

Donc : $A = 2(X + 1)^3 \left(X - \frac{1}{2}\right) (X^2 + 1)^2$ est la décomposition de A en facteurs irréductibles unitaires dans $\mathbb{R}[X]$.

$A = 2(X + 1)^3 \left(X - \frac{1}{2}\right) (X - i)^2 (X + i)^2$ est la décomposition de A en facteurs irréductibles unitaires dans $\mathbb{C}[X]$.

- 2^{ème} méthode :

En utilisant le procédé de Hôrner on a vu que :

i) -1 est une racine de A d'ordre de multiplicité 3 et que

$A_1 = 2X^5 - X^4 + 4X^3 - 2X^2 + 2X - 1$ est le quotient de la division euclidienne de A par $(X + 1)^3$.

ii) $\frac{1}{2}$ est une racine simple de A et que $A_2 = 2X^4 + 4X^2 + 2$ est le quotient de la division euclidienne de A_1 par $X - \frac{1}{2}$.

$$\begin{aligned}
\text{Alors : } A &= (X+1)^3 A_1 = (X+1)^3 \left(X - \frac{1}{2}\right) A_2 = (X+1)^3 \left(X - \frac{1}{2}\right) (2X^4 + 4X^2 + 2) \\
&= (X+1)^3 \left(X - \frac{1}{2}\right) 2(X^4 + 2X^2 + 1) \\
&= 2(X+1)^3 \left(X - \frac{1}{2}\right) (X^2 + 1)^2 \\
&= 2(X+1)^3 \left(X - \frac{1}{2}\right) (X-i)^2 (X+i)^2.
\end{aligned}$$

Donc : $A = 2(X+1)^3 \left(X - \frac{1}{2}\right) (X^2 + 1)^2$ est la décomposition de A en facteurs irréductibles unitaires dans $\mathbb{R}[X]$.

$A = 2(X+1)^3 \left(X - \frac{1}{2}\right) (X-i)^2 (X+i)^2$ est la décomposition de A en facteurs irréductibles unitaires dans $\mathbb{C}[X]$.

- 3^{ième} méthode :

Par la méthode des dérivées successives et la méthode du procédé de Hôrner on a vu que $-1, \frac{1}{2}, i$ et $-i$ sont des racines de A d'ordres de multiplicité 3, 1, 2 et 2.

Alors les polynômes $(X+1)^3, X - \frac{1}{2}, (X-i)^2$ et $(X+i)^2$ sont des diviseurs de A .

Donc le produit $B = (X+1)^3 \left(X - \frac{1}{2}\right) (X-i)^2 (X+i)^2$ est un diviseur de A .

$$\begin{cases} B|A \\ d^0 B = 8 = d^0 A \end{cases} \Rightarrow A \sim B \Rightarrow \exists \alpha \in \mathbb{C} \text{ tq : } A = \alpha B.$$

Puisque le polynôme B est unitaire alors $\alpha = 2$ est le coefficient dominant de A .

$$\begin{aligned}
\text{Donc : } A &= 2B = 2(X+1)^3 \left(X - \frac{1}{2}\right) (X-i)^2 (X+i)^2 \\
&= 2(X+1)^3 \left(X - \frac{1}{2}\right) (X^2 + 1)^2
\end{aligned}$$

Alors : $A = 2(X+1)^3 \left(X - \frac{1}{2}\right) (X-i)^2 (X+i)^2$ est la décomposition de A en facteurs irréductibles unitaires dans $\mathbb{C}[X]$.

$A = 2(X+1)^3 \left(X - \frac{1}{2}\right) (X^2 + 1)^2$ est la décomposition de A en facteurs irréductibles unitaires dans $\mathbb{R}[X]$.

Théorème 4-7-7 :

Soient A et B deux polynômes à coefficients dans K , $P_1, P_2, \dots, P_n$ des polynômes irréductibles dans $K[X]$ non associés deux à deux, $\alpha_1, \alpha_2, \dots, \alpha_n, \beta_1, \beta_2, \dots, \beta_n$ des entiers naturels et $a, b \in K^*$.

Si $\begin{cases} A = aP_1^{\alpha_1} P_2^{\alpha_2} \dots P_n^{\alpha_n} \\ B = bP_1^{\beta_1} P_2^{\beta_2} \dots P_n^{\beta_n} \end{cases}$ alors les trois propriétés suivantes sont vérifiées :

i) $A|B \Leftrightarrow [\forall k = 1, 2, \dots, n : \alpha_k \leq \beta_k]$.

ii) $P_1^{\min(\alpha_1, \beta_1)} P_2^{\min(\alpha_2, \beta_2)} \dots P_n^{\min(\alpha_n, \beta_n)}$ est un p.g.c.d de A et B

où $\min(\alpha_k, \beta_k)$ est le minimum des deux entiers naturels α_k et β_k pour tout entier naturel $k = 1, 2, \dots, n$.

iii) $P_1^{\max(\alpha_1, \beta_1)} P_2^{\max(\alpha_2, \beta_2)} \dots P_n^{\max(\alpha_n, \beta_n)}$ est un p.p.c.m de A et B .

où $\max(\alpha_k, \beta_k)$ est le maximum des deux entiers naturels α_k et β_k pour tout entier naturel $k = 1, 2, \dots, n$.

iv) Si de plus $P_1, P_2, \dots, P_n$ sont unitaires alors on a :

$$\begin{cases} A \wedge B = P_1^{\min(\alpha_1, \beta_1)} P_2^{\min(\alpha_2, \beta_2)} \dots P_n^{\min(\alpha_n, \beta_n)} \\ A \vee B = P_1^{\max(\alpha_1, \beta_1)} P_2^{\max(\alpha_2, \beta_2)} \dots P_n^{\max(\alpha_n, \beta_n)} \end{cases} .$$

Démonstration :

Supposons qu'on a : $\begin{cases} A = aP_1^{\alpha_1} P_2^{\alpha_2} \dots P_n^{\alpha_n} \\ B = bP_1^{\beta_1} P_2^{\beta_2} \dots P_n^{\beta_n} \end{cases}$. Alors, d'après le théorème 4-7-1 :

$$\begin{cases} \alpha_1, \alpha_2, \dots, \alpha_n \text{ sont les ordres de multiplicité respectivement de } P_1, P_2, \dots, P_n \text{ dans } A \\ \beta_1, \beta_2, \dots, \beta_n \text{ sont les ordres de multiplicité respectivement de } P_1, P_2, \dots, P_n \text{ dans } B \end{cases} .$$

i) $\Rightarrow$) **Si A est un diviseur de B :**

Soient $k = 1, 2, \dots, n$ quelconque.

$$\begin{cases} P_k^{\alpha_k} | A \\ A | B \end{cases} \Rightarrow P_k^{\alpha_k} | B \Rightarrow \alpha_k \leq \beta_k \text{ (car } \beta_k \text{ est l'ordre de multiplicité de } P_k \text{ dans } B).$$

On a donc montrer que pour tout entier naturel $k = 1, 2, \dots, n : \alpha_k \leq \beta_k$.

$\Leftarrow$) **Si on a pour tout entier naturel $k = 1, 2, \dots, n : \alpha_k \leq \beta_k$:**

$$\begin{aligned} B &= bP_1^{\beta_1} P_2^{\beta_2} \dots P_n^{\beta_n} = a a^{-1} b P_1^{\alpha_1 - \alpha_1 + \beta_1} P_2^{\alpha_2 - \alpha_2 + \beta_2} \dots P_n^{\alpha_n - \alpha_n + \beta_n} \\ &= a a^{-1} b P_1^{\alpha_1} P_1^{\beta_1 - \alpha_1} P_2^{\alpha_2} P_2^{\beta_2 - \alpha_2} \dots P_n^{\alpha_n} P_n^{\beta_n - \alpha_n} \\ &= (a P_1^{\alpha_1} P_2^{\alpha_2} \dots P_n^{\alpha_n}) (a^{-1} b P_1^{\beta_1 - \alpha_1} P_2^{\beta_2 - \alpha_2} \dots P_n^{\beta_n - \alpha_n}) \\ &= A \cdot (a^{-1} b P_1^{\beta_1 - \alpha_1} P_2^{\beta_2 - \alpha_2} \dots P_n^{\beta_n - \alpha_n}). \end{aligned}$$

Donc A est un diviseur de B.

Ce qui montre que : $A | B \Leftrightarrow [\forall k = 1, 2, \dots, n : \alpha_k \leq \beta_k]$.

ii) Posons $D = P_1^{\min(\alpha_1, \beta_1)} P_2^{\min(\alpha_2, \beta_2)} \dots P_n^{\min(\alpha_n, \beta_n)}$.

$$\star \begin{cases} \forall k = 1, 2, \dots, n : \min(\alpha_k, \beta_k) \leq \alpha_k \\ \forall k = 1, 2, \dots, n : \min(\alpha_k, \beta_k) \leq \beta_k \end{cases} \Rightarrow \begin{cases} D | A \\ D | B \end{cases} .$$

Donc D est un diviseur commun de A et B.

$\star$ Soit Δ un diviseur commun quelconque de A et B.

Puisque Δ un diviseur de A alors (d'après le théorème 4-7-2) il existe un élément non nul d de K et des entiers naturels $\gamma_1, \gamma_2, \dots, \gamma_n$ tels que $\Delta = d P_1^{\gamma_1} P_2^{\gamma_2} \dots P_n^{\gamma_n}$.

$$\begin{aligned} \begin{cases} \Delta | A \\ \Delta | B \end{cases} &\Rightarrow \begin{cases} \forall k = 1, 2, \dots, n : \gamma_k \leq \alpha_k \\ \forall k = 1, 2, \dots, n : \gamma_k \leq \beta_k \end{cases} \Rightarrow [\forall k = 1, 2, \dots, n : \gamma_k \leq \min(\alpha_k, \beta_k)] \\ &\Rightarrow \Delta | D. \end{aligned}$$

Donc Δ est un diviseur de D.

Ce qui montre que $P_1^{\min(\alpha_1, \beta_1)} P_2^{\min(\alpha_2, \beta_2)} \dots P_n^{\min(\alpha_n, \beta_n)} = D$ est un p.g.c.d de A et B.

iii) Posons $M = P_1^{\max(\alpha_1, \beta_1)} P_2^{\max(\alpha_2, \beta_2)} \dots P_n^{\max(\alpha_n, \beta_n)}$.

$$\star \begin{cases} \forall k = 1, 2, \dots, n : \alpha_k \leq \max(\alpha_k, \beta_k) \\ \forall k = 1, 2, \dots, n : \beta_k \leq \max(\alpha_k, \beta_k) \end{cases} \Rightarrow \begin{cases} A | M \\ B | M \end{cases} .$$

Donc M est un multiple commun de A et B.

★ Soit N un multiple commun quelconque de A et B .

$\forall k = 1, 2, \dots, n :$

$$\left\{ \begin{array}{l} P_k^{\alpha_k} | A \\ A | N \end{array} \right\} \Rightarrow P_k^{\alpha_k} | N \quad \text{et} \quad \left\{ \begin{array}{l} P_k^{\beta_k} | B \\ B | N \end{array} \right\} \Rightarrow P_k^{\beta_k} | N.$$

Puisque $P_1^{\max(\alpha_1, \beta_1)}, P_2^{\max(\alpha_2, \beta_2)}, \dots, P_n^{\max(\alpha_n, \beta_n)}$ sont des diviseurs communs de N , distincts deux à deux alors $P_1^{\max(\alpha_1, \beta_1)} P_2^{\max(\alpha_2, \beta_2)} \dots P_n^{\max(\alpha_n, \beta_n)} = M$ est un diviseur de N .

Donc N est un multiple de M

Ce qui montre que $P_1^{\max(\alpha_1, \beta_1)} P_2^{\max(\alpha_2, \beta_2)} \dots P_n^{\max(\alpha_n, \beta_n)} = M$ est un *p.p.c.m* de A et B .

iv) Si de plus $P_1, P_2, \dots, P_n$ sont unitaires :

$$\left\{ \begin{array}{l} P_1^{\min(\alpha_1, \beta_1)} P_2^{\min(\alpha_2, \beta_2)} \dots P_n^{\min(\alpha_n, \beta_n)} \text{ est un } p.g.c.d \text{ unitaire de } A \text{ et } B \\ P_1^{\max(\alpha_1, \beta_1)} P_2^{\max(\alpha_2, \beta_2)} \dots P_n^{\max(\alpha_n, \beta_n)} \text{ est un } p.p.c.m \text{ unitaire de } A \text{ et } B \end{array} \right.$$

$$\text{Par suite on a : } \left\{ \begin{array}{l} A \wedge B = P_1^{\min(\alpha_1, \beta_1)} P_2^{\min(\alpha_2, \beta_2)} \dots P_n^{\min(\alpha_n, \beta_n)} \\ A \vee B = P_1^{\max(\alpha_1, \beta_1)} P_2^{\max(\alpha_2, \beta_2)} \dots P_n^{\max(\alpha_n, \beta_n)} \end{array} \right.$$

Exemples 4-7-8 :

Dans $\mathbb{R}[X]$:

$$\star \text{ Si } \left\{ \begin{array}{l} A = 3(2X+5)^3(X-3)(5X-4)^5(2X^2+1)^2 \\ B = 2(2X+5)^4(X-3)^5(X+2)^2(5X-4)^5(2X^2+1)^3 \end{array} \right.$$

$$\text{On a alors : } \left\{ \begin{array}{l} A = 3(2X+5)^3(X-3)^1(X-3)^0(5X-4)^5(2X^2+1)^2 \\ B = 2(2X+5)^4(X-3)^5(X+2)^2(5X-4)^5(2X^2+1)^3 \end{array} \right.$$

Donc : $A|B$

$$\begin{aligned} & (2X+5)^3(X-3)^1(X-3)^0(5X-4)^5(2X^2+1)^2 \\ &= (2X+5)^3(X-3)(5X-4)^5(2X^2+1)^2 \text{ est un } p.g.c.d \text{ de } A \text{ et } B. \\ & (2X+5)^4(X-3)^5(X+2)^2(5X-4)^5(2X^2+1)^3 \text{ est un } p.p.c.m \text{ de } A \text{ et } B. \\ & \text{est un } p.p.c.m \text{ de } A \text{ et } B. \end{aligned}$$

$$\star \text{ Si } \left\{ \begin{array}{l} A = 7(X+5)^4(X-3)(2X-4)^5(X^2+1)^2(2X^2+1)^3 \\ B = 2(X+5)^2(X-3)(5X-4)^3(2X^2+1)^2 \end{array} \right.$$

$$\text{On a alors : } \left\{ \begin{array}{l} A = 7(X+5)^4(X-3)^1(2X-4)^5(X^2+1)^2(2X^2+1)^3 \\ B = 2(X+5)^2(X-3)^1(2X-4)^3(X^2+1)^0(2X^2+1)^2 \end{array} \right.$$

Donc : $B|A$

$$\begin{aligned} & (X+5)^2(X-3)^1(2X-4)^3(X^2+1)^0(2X^2+1) \\ &= (X+5)^2(X-3)(2X-4)^3(2X^2+1)^2 \text{ est un } p.g.c.d \text{ de } A \text{ et } B. \\ & (X+5)^4(X-3)(2X-4)^5(X^2+1)^2(2X^2+1)^3 \text{ est un } p.p.c.m \text{ de } A \text{ et } B. \end{aligned}$$

$$\star \text{ Si } \begin{cases} A = 3(X+5)^4(X-3)(2X-4)^2(2X^2+1)^3 \\ B = 5(X+5)^2(2X-4)^3(X^2+1)^5(2X^2+1) \end{cases} .$$

$$\text{On a alors : } \begin{cases} A = 3(X+5)^4(X-3)^1(2X-4)^2(X^2+1)^0(2X^2+1)^3 \\ B = 5(X+5)^2(X-3)^0(2X-4)^3(X^2+1)^5(2X^2+1) \end{cases}$$

Donc : $A \nmid B$ et $B \nmid A$

$$(X+5)^2(X-3)^0(2X-4)^2(X^2+1)^0(2X^2+1)^1 = (X+5)^2(2X-4)^2(2X^2+1)$$

est un *p.g.c.d* de A et B .

$$(X+5)^4(X-3)(2X-4)^3(X^2+1)^5(2X^2+1)^3 \text{ est un } p.p.c.m \text{ de } A \text{ et } B.$$

$$\star \text{ Si } \begin{cases} A = 3(X+5)^4(X-3)(X-4)^2(X^2+X+3)^3 \\ B = 5(X+5)^2(X-4)^3(X^2+1)^3(2X^2+1) \end{cases} .$$

$$\text{Alors : } \begin{cases} A = 3(X+5)^4(X-3)^1(X-4)^2(X^2+1)^0(X^2+X+3)^3 \\ B = 5(X+5)^2(X-3)^0(X-4)^3(X^2+1)^3(2X^2+1)^1 \end{cases} .$$

Donc : $A \nmid B$ et $B \nmid A$

$$\begin{aligned} A \wedge B &= (X+5)^2(X-3)^0(X-4)^2(X^2+1)^0(X^2+X+3)^1 \\ &= (X+5)^2(X-4)^2(X^2+X+3). \end{aligned}$$

$$A \vee B = (X+5)^4(X-3)(X-4)^3(X^2+1)^3(X^2+X+3)^3.$$